UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera de Ingeniería en Sistemas Computacionales

IDENTIFICACIÓN DE VULNERABILIDADES DE LOS SERVICIOS TECNOLÓGICOS DE LA UNIÓN DE COOPERATIVAS DE AHORRO Y CRÉDITO DEL NORTE APLICANDO LA PRÁCTICA DE PENTESTING.

Trabajo de grado presentado ante la Ilustre Universidad Técnica del Norte previo a la obtención del título de Ingeniero en Sistemas Computacionales

Autor:

Carlos Guillermo Erazo Bastidas

Directora:

Ing. Cathy Guevara

Ibarra – Ecuador

Septiembre 2017

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1 IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto de Repositorio Digital Institucional, determina la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

CÉDULA DE IDENTIDAD:	1717538266
NOMBRES:	CARLOS GUILLERMO ERAZO BASTIDAS
DIRECCIÓN:	SAN ANTONIO
E-MAIL:	cgerazo@utn.edu.ec
TELÉFONO FIJO:	062932814
TELÉFONO MÓVIL:	0981991456

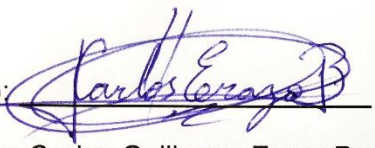
DATOS DE LA OBRA	
TÍTULO:	“IDENTIFICACIÓN DE VULNERABILIDADES DE LOS SERVICIOS TECNOLÓGICOS DE LA UNIÓN DE COOPERATIVAS DE AHORRO Y CRÉDITO DEL NORTE APLICANDO LA PRÁCTICA DE PENTESTING”
AUTOR:	CARLOS GUILLERMO ERAZO BASTIDAS
FECHA:	3 de agosto del 2017
PROGRAMA:	PREGRADO
TÍTULO POR EL QUE OPTA:	INGENIERÍA EN SISTEMAS COMPUTACIONALES
DIRECTORA:	ING. CATHY GUEVARA, MSc.

2 AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, CARLOS GUILLERMO ERAZO BASTIDAS, con cédula de identidad Nro. 1717538266, en calidad de autor y titular de los derechos patrimoniales del trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación del trabajo en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

3 CONSTANCIA

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asumo la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

(Firma): 

Nombre: Carlos Guillermo Erazo Bastidas

Cédula: 171753826-6

Ibarra, 3 de agosto de 2017

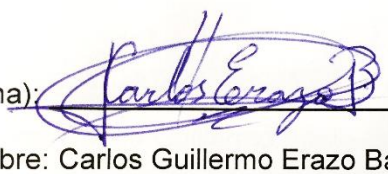
UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, CARLOS GUILLERMO ERAZO BASTIDAS con cédula de identidad Nro. 1717538266, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4,5,6, en calidad de autor de trabajo de grado denominado **"IDENTIFICACIÓN DE VULNERABILIDADES DE LOS SERVICIOS TECNOLÓGICOS DE LA UNIÓN DE COOPERATIVAS DE AHORRO Y CRÉDITO DEL NORTE APLICANDO LA PRÁCTICA DE PENTESTING"**, que ha sido desarrollado para optar por el título de Ingeniero en Sistemas Computacionales, en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos concedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

(Firma): 

Nombre: Carlos Guillermo Erazo Bastidas

Cédula: 171753826-6

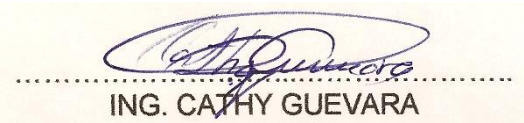
Ibarra, 3 de agosto de 2017

UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

CERTIFICACIÓN DIRECTORA

Certifico que el trabajo de grado “IDENTIFICACIÓN DE VULNERABILIDADES DE LOS SERVICIOS TECNOLÓGICOS DE LA UNIÓN DE COOPERATIVAS DE AHORRO Y CRÉDITO DEL NORTE APLICANDO LA PRÁCTICA DE PENTESTING”, ha sido desarrollado en su totalidad por el señor: Carlos Guillermo Erazo Bastidas portador de la cédula de identidad número: 171753826-6.



ING. CATHY GUEVARA

DIRECTORA DE TRABAJO DE GRADO

Olmedo 1-23 y Villamar
062-611 809 / 062-611 389
gerencia@ucacnor.org// secretaria@ucacnor.org
www.ucacnor.org
LA FUERZA DEL NORTE DEL PAÍS

UNIÓN DE COOPERATIVAS DE AHORRO Y CRÉDITO DEL NORTE
UCACNOR
LA FUERZA DEL NORTE DEL PAÍS

CERTIFICADO DE IMPLEMENTACIÓN DEL PRODUCTO DEL PROYECTO DE TRABAJO DE GRADO

La Unión de Cooperativas de Ahorro y Crédito del Norte **"UCACNOR"**

C E R T I F I C A :

Que, siendo auspiciantes del proyecto de grado del Sr. **CARLOS GUILLERMO ERAZO BASTIDAS**, portador de la cédula de identidad número 171753826-6 quien desarrolló su proyecto de grado: **IDENTIFICACIÓN DE VULNERABILIDADES DE LOS SERVICIOS TECNOLÓGICOS DE LA UNIÓN DE COOPERATIVAS DE AHORRO Y CRÉDITO DEL NORTE APLICANDO LA PRÁCTICA DE PENTESTING**, me es grato informar que ha superado a satisfacción las pruebas técnicas y la revisión del cumplimiento de los términos del test de intrusión (pentesting), por lo que se recibe el proyecto como culminado e implementado en su totalidad.

El Sr. CARLOS GUILLERMO ERAZO BASTIDAS puede hacer uso de este documento para los fines pertinentes en la Universidad Técnica del Norte.

Es todo cuanto certifico, en honor a la verdad y para los fines que correspondan.

Ibarra, julio 12 del 2017.

Ing. Rommel Alarcón
Gerente General UCACNOR

UCACNOR
La fuerza del norte del país

GERENCIA
UCACNOR

DEDICATORIA

Quiero dedicar el presente trabajo principalmente a Dios ya que me ha llenado de bendiciones y de vida, elementos fundamentales para poder finalizar mi etapa universitaria de la mejor manera.

A mi querida madre Gloria Bastidas, por haberme guiado siempre por el camino del bien y quien con toda su sabiduría y paciencia ha sabido brindarme infinitas enseñanzas que hoy se ven reflejadas en este gran logro obtenido.

A mis queridos primos Pablo, Lorena, Paulina y Gabriela Cruz, quienes siempre me han brindado todo su cariño y apoyo para culminar este trabajo.

Carlos.

AGRADECIMIENTOS

Deseo agradecer a Dios por haberme bendecido y dado fuerzas para concluir este largo camino universitario.

A mi querida Madre y Familia, por haber estado apoyándome incondicionalmente siempre y especialmente en los momentos que más los he necesitado.

A la Ing. Cathy Guevara por su incalculable ayuda y guía en todo el desarrollo de este trabajo, sin sus conocimientos y orientación no lo hubiese logrado.

A todos quienes conforman la Unión de Cooperativas de Ahorro y Crédito del Norte “UCACNOR”, por haberme dado la oportunidad y su colaboración al momento de realizar este proyecto.

Gracias a todos ustedes.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

Resumen

Los delitos informáticos cada vez son más elaborados y peligrosos ya sea en el ámbito empresarial o personal, por lo tanto, es necesario tomar medidas proactivas para proteger adecuadamente los activos tecnológicos que se posee.

La presente investigación se desarrolló con la finalidad de solventar las sospechas y preocupaciones de ataques e intrusiones no autorizadas a varios servicios tecnológicos en una organización, además, fue diseñada para promover la protección proactiva de sus activos tecnológicos, evaluando su nivel de seguridad mediante una serie de pruebas específicas.

El Pentesting llevado a cabo hace uso de una metodología sintetizada, pero a la vez muy completa, adecuada completamente al escenario empresarial. Su desarrollo se ejecutó en cinco fases secuenciales, con diferentes objetivos específicos, pero con un mismo objetivo final.

Al finalizar el trabajo se obtuvieron los resultados esperados, mismos que se enfocan principalmente en la identificación de vulnerabilidades y la emisión de recomendaciones útiles para la corrección anticipada de las mismas, antes de su explotación con fines maliciosos.

Palabras claves

Seguridad informática, Pentesting, Test de intrusión, Hacker, Vulnerabilidades, Auditoría informática, Riesgos informáticos.

Abstract

Computer crimes are becoming more elaborate and dangerous in the business or personal, therefore, it is necessary to take proactive measures to adequately protect the technological assets that are owned.

The present investigation was developed with the purpose of solving the suspicions and concerns of unauthorized attacks and intrusions to several technological services in an organization. In addition, it was designed to promote the proactive protection of its technological assets, evaluating its level of security through a series of specific tests.

The Pentesting carried out uses a methodology synthesized, but at the same time very complete, completely adequate to the business scenario. Its development was executed in five sequential phases, with different specific objectives, but with the same final objective.

At the end of the work, the expected results were obtained, which are mainly focused on the identification of vulnerabilities and the issuance of useful recommendations for the early correction of the vulnerabilities, prior to their exploitation for malicious purposes.

Keywords

Computer security, Pentesting, Intrusion test, Hacker, Vulnerabilities, Computer audit, Computer risks.

Introducción

Antecedentes

Desde el año 1980 el mundo ha venido escuchando temas relacionados con la Seguridad Informática, y es uno de sus pioneros, James P. Anderson quien, en el mismo año, escribió uno de los documentos más acertados en cuanto a seguridad informática se refiere, en el cual define la gran importancia del comportamiento enfocado hacia la seguridad en materia de informática (Pérez, 2015).

Posteriormente en el año 1983 aparece el primer virus experimental capaz de modificar el código de un programa con el objetivo de realizar una copia de sí mismo e incluirse en el software atacado, todo esto para incrementar su propagación y expansión (Weidman, 2014).

En el año 1998 debido a los problemas causados por el gusano informático llamado Morris, fue necesaria la creación de un organismo de control en temas relacionados a la seguridad informática, desde entonces el CERT (Computer Emergency Response Team) Coordination Center, se ha convertido en un centro de coordinación mundial sobre problemas de seguridad informática, receptando vulnerabilidades de investigadores a nivel mundial (SoftDoit, 2016).

Por lo tanto, este campo de la informática se ha venido desarrollando considerablemente, al punto que en la actualidad se encuentra carreras de estudio netamente enfocadas en la seguridad informática.

Situación actual

La seguridad informática se considera como uno de los aspectos más críticos dentro de una empresa o institución, debido a que, gracias a esta sus datos e información entera se mantendrían seguros y resguardados, sin embargo, en la mayoría de instituciones del Ecuador este aspecto no ha sido tomado muy en cuenta, lo cual, pone en riesgo la información manejada por medios tecnológicos de las mismas.

Actualmente, los ataques informáticos han crecido exponencialmente debido a la digitalización de la información en las empresas, por lo tanto, existen muchos casos de ataques a organizaciones, las cuales sufren incidentes que podrían haberse evitado si los mecanismos de protección a la información hubiesen sido proactivos. Uno de estos mecanismos es el Pentesting o Test de penetración, el cual consiste en la realización de

pruebas ofensivas en contra de los mecanismos de defensa existentes en el entorno analizado.

Prospectiva

Con esta investigación se logrará identificar los puntos débiles o vulnerabilidades existentes en los servicios tecnológicos de una institución, simulando posibles ataques de un cibercriminal en un ambiente controlado, para posteriormente corregir proactivamente dichas fallas y evitar poner en riesgo información de una institución.

El aporte que proveerá esta investigación a la Carrera de Ingeniería en Sistemas Computacionales (CISIC) de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) perteneciente a la Universidad Técnica del Norte (UTN), será el desarrollo de un test de penetración en un determinado servicio tecnológico, explicando las diferentes técnicas que implica realizarlo y de esta forma impulsar el estudio sobre la rama de Seguridad informática.

Descripción del problema

¿Cómo identificar las vulnerabilidades informáticas en los servicios tecnológicos de la Unión de Cooperativas de Ahorro y Crédito del Norte?

La infraestructura tecnológica dentro de una empresa, así como sus sistemas informáticos han comenzado a ser un objetivo muy llamativo para los cibercriminales debido a la importancia de la información manejada por estas vías, por lo tanto, en la actualidad las amenazas a nivel digital son demasiado críticas, pudiendo comprometer el sigilo y privacidad de la organización o inclusive de sus trabajadores.

Los robos de información digital y en general el cibercrimen son negocios muy lucrativos hoy por hoy, inclusive se ha llegado a comprobar que estos producen más dinero que el narcotráfico, por lo tanto, es de vital importancia un estudio que contribuya a la protección tecnológica tanto en los pasivos, como activos de una empresa.

La Unidad de Tecnologías de la Información y Comunicación (TICs) de la Unión de Cooperativas de Ahorro y Crédito del Norte (UCACNOR), ha visto muy necesaria la realización de un Pentesting a sus medios tecnológicos, debido a la creciente preocupación de esta entidad a varias sospechas de ataques e intromisiones, pudiendo comprometer información crítica perteneciente a la organización y sus intereses.

Cualquier medio o equipo tecnológico conectado a internet siempre sufrirá ataques informáticos, la diferencia se marca en si este está o no preparado para defenderse

eficazmente, por lo tanto la práctica de Pentesting a desarrollarse ayudará a comprobar y mejorar el nivel de seguridad de los servicios tecnológicos de la UCACNOR, por medio de ataques informáticos controlados identificando las vulnerabilidades por las que un cibercriminal podría acceder y dañar la información contenida en los equipos informáticos de la organización.

Justificación

Actualmente los servicios e infraestructuras tecnológicas son las más atacadas en una organización, esto se debe a la información vital que contienen, por tal motivo, es sumamente necesario proteger y controlar de una manera óptima los procesos que manejen dicha información.

Uno de los parámetros principales al momento de proteger la información es la identificación de vulnerabilidades en la mayoría de medios tecnológicos presentes en la organización, por lo tanto, ejecutar la práctica de pentesting constantemente debería ser una prioridad alta en la política de una empresa.

Este trabajo busca determinar y aplicar las principales líneas de defensa en sistemas informáticos por medio de la exploración e identificación de fallas o vulnerabilidades que pueden estar presentes en los medios tecnológicos de una organización, para posteriormente presentar dos informes donde se detallen los problemas encontrados y las recomendaciones para solucionarlos; de esta manera, se incrementará notablemente la seguridad informática dentro de la organización, evitando accesos no autorizados, robos, alteración, espionaje o borrado de información confidencial.

La presente investigación corresponde a una justificación tecnológica debido a que resuelve problemas relacionados a fallos y vulnerabilidades presentes en medios tecnológicos. Además, propone las posibles soluciones a los errores de seguridad encontrados, intentando proteger proactivamente la información en medios digitales de la Unión de Cooperativas de Ahorro y Crédito, adicionalmente, este trabajo fortalecerá el know how de la Unidad de TICs de la organización, la cual se encarga de garantizar el correcto funcionamiento de los equipos informáticos internos, en base a los requerimientos tecnológicos de las demás unidades, así como también proteger la información digital de las mismas.

Tanto las técnicas y/o herramientas mostradas en esta investigación tienen propósitos estrictamente educativos e investigativos, no es responsabilidad del autor de esta investigación el mal uso de las mismas.

Objetivos

Objetivo General

Identificar las vulnerabilidades de los servicios tecnológicos para mejorar la seguridad informática de la Unión de Cooperativas de Ahorro y Crédito del Norte aplicando la práctica de Pentesting.

Objetivos Específicos

- Identificar y determinar con los responsables de la Unión de Cooperativas de Ahorro y Crédito los servicios tecnológicos que serán analizados.
- Verificar las seguridades informáticas actuales de los servicios tecnológicos a evaluarse.
- Aplicar el Pentesting para identificar las vulnerabilidades existentes, y de esta forma proteger proactivamente la información almacenada en medios tecnológicos en la Unión de Cooperativas de Ahorro y Crédito.
- Presentar el informe de resultados del Pentesting realizado con las vulnerabilidades encontradas.

Alcance

Esta investigación ayudará a identificar los fallos y problemas de seguridad en el aspecto tecnológico de la Unión de Cooperativas de Ahorro y Crédito, así como las respectivas recomendaciones para solucionarlos, por lo tanto, esta investigación generará un Informe de Pentesting.

Para realizar el examen de penetración planteado en esta institución, se realizarán las siguientes fases:

Ilustración 0.1 Fases del Pentesting.
Fuente: https://www.dragonjar.education/leccion/introduccion-al-pentesting-metodologia/

Fase de Recolección de información: también es conocida como “reconocimiento” y es una de las etapas más importantes del Pentesting. En esta se definirán los medios tecnológicos objetivo de la organización y se recopilará la mayor cantidad de información pública posible, misma que será de gran ayuda en las etapas posteriores. La información que se buscará abarca principalmente desde nombres y direcciones de correo de los empleados de la organización, hasta la búsqueda de metadatos en su sitio web.

Fase de Enumeración: es complementaria a la etapa anterior debido a que se seguirá recopilando información sobre el objetivo, pero con la gran diferencia de que en esta ya se interactúa directamente con los activos tecnológicos de la organización auditada. Esta fase buscará principalmente la detección de direcciones IP, equipos, puertos y servicios pertenecientes a UCACNOR.

Fase de Análisis: esta etapa se caracteriza por efectuar un contacto directo y posiblemente agresivo con los activos tecnológicos de la organización, por lo tanto, es de vital importancia contar con la autorización y los permisos adecuados por parte de la organización auditada para efectuar los procedimientos de análisis. En esta etapa se utilizará la información antes obtenida para ejecutar varios escáneres de vulnerabilidades y posteriormente se expondrá las posibles fallas encontradas en los medios analizados, mismas que permitirán definir los vectores de ataque a explotar en la siguiente fase.

Fase de Explotación: en esta etapa se realizarán ataques intrusivos y directos a un objetivo en específico, esta tarea se consigue a partir del aprovechamiento de las vulnerabilidades encontradas en etapas anteriores, mismas que serán utilizadas por el auditor para comprometer varios activos tecnológicos de la organización.

Fase de Documentación: finalmente, a partir de los resultados obtenidos se generará la documentación correspondiente con los detalles que comprendieron la auditoría, en los cuales es importante indicar las medidas necesarias para evitar que la organización sufra ataques e incidentes por parte de cibercriminales reales. Se generarán dos informes (ejecutivo y técnico) sobre los resultados del Pentesting; además se realizarán dos capacitaciones sobre seguridad informática al personal de UCACNOR, con el objetivo de fortalecer la parte más susceptible a ataques cibernéticos en una organización.

Cabe destacar que la seguridad debe ser gestionada proactivamente, contemplando la necesidad de la realización de auditorías de este tipo constantemente.

CAPÍTULO 1

Revisión Bibliográfica

1.1 Seguridad Informática

La Seguridad informática (SI) es un conjunto de técnicas y herramientas enfocadas en la protección de la infraestructura computacional y la información que esta contiene, es decir, todos los activos tecnológicos y afines de la empresa como por ejemplo equipos de computación, impresoras, servidores, routers, firewalls y sistemas de detección de intrusos.

Para cumplir con su objetivo la SI cuenta con una serie de estándares, protocolos, métodos, reglas, herramientas y leyes para minimizar los posibles riesgos a los cuales dichos activos estarían expuestos. Además, la seguridad informática engloba tanto el software como hardware de los dispositivos tecnológicos, por lo tanto, la SI se encarga de velar por la integridad física y lógica del activo (DAIT Seguridad Informática, 2015).

La seguridad informática está concebida específicamente para proteger los activos informáticos, descritos a continuación:

La información: es el activo con mayor importancia dentro de una empresa, la cual se almacena y maneja en la infraestructura computacional utilizada por los usuarios, por lo tanto, la SI tiene como objetivo prioritario velar y cuidar de esta. La información por proteger puede estar presente en varios escenarios como, por ejemplo: credenciales de autentificación de usuarios, información bancaria, bases de datos y archivos. Por lo tanto, si la información confidencial llegara a manos de personas no autorizadas, se convertiría en un riesgo potencial para la organización (DAIT Seguridad Informática, 2015).

La infraestructura tecnológica: son todos los dispositivos tecnológicos con los que cuenta la organización, la SI tiene como objetivo custodiar el correcto funcionamiento de los mismos, así como también prevenir, mediante planes de contingencia, las fallas, ataques informáticos, sabotajes o cualquier otro factor que atente en contra de la integridad de estos (DAIT Seguridad Informática, 2015).

Los usuarios: son las personas que utilizan la plataforma tecnológica de una organización para gestionar la información. Los usuarios son una de las principales causas de inseguridad dentro de una empresa, ya que la tecnología en muchos de los casos fue construida sin pensar en el usuario sin conocimientos técnicos en el campo de la informática, por lo que, debido a esto es sumamente necesaria la educación en seguridad informática a todo el personal dentro de una organización. Además, todos los sistemas deben protegerse para que

el uso por parte de ellos no pueda comprometer la seguridad de la información (DAIT Seguridad Informática, 2015).

En resumen, la Seguridad Informática se encarga de las implementaciones técnicas para la protección de la información; y de esta manera prevenir, detectar y corregir, anomalías e incidentes que puedan comprometer la integridad, disponibilidad, confidencialidad y autenticidad de la información. La familia de normas ISO/IEC 27000 es la más relacionada con la seguridad informática.

Ilustración 1.1 Pilares principales de la seguridad informática.
Fuente: Propia.

1.2 Ethical Hacking

En la actualidad no existe empresa que pueda prescindir del internet, medio que se ha vuelto indispensable en la mayoría de procesos y acciones críticas realizadas a menudo por estas, pero además de ser un canal de comunicación muy útil, el internet también puede convertirse en uno de los mayores peligros, ya que si no se aplica una correcta política de seguridad informática empresarial y no se aplica una configuración adecuada a los elementos de protección, todos sus activos podrían quedar expuestos a innumerables amenazas presentes en dicho medio.

El Ethical Hacking o Hacking ético nació con la finalidad de ayudar en la defensa y protección de los activos tecnológicos de gobiernos, empresas y organizaciones, velando por la confidencialidad, integridad y disponibilidad de dichos activos, para lo cual, el Hacking ético realiza varias pruebas bajo el consentimiento y conocimiento del cliente, con el objetivo de descubrir vulnerabilidades o fallos de seguridad que puedan llegar a significar hasta el más mínimo riesgo para la empresa y sus operaciones (González Pérez, 2014).

Un hacker ético procura utilizar las mismas herramientas o metodologías que un cibercriminal, realizando simulaciones de un ataque real; con el objetivo de descubrir y corregir posibles vulnerabilidades en la infraestructura tecnológica de una empresa, antes de

que sean utilizadas por usuarios maliciosos. Por último, el hacker ético debe realizar un informe minucioso de los resultados obtenidos, para que los directivos de la organización entiendan la necesidad de mejorar la seguridad informática y los peligros que conllevaría no hacerlo (González Pérez, 2014).

Dentro del Ethical Hacking el Pentesting es el encargado de comprobar y evaluar la seguridad física y lógica de los activos empresariales, desde los equipos de computación, la red, los sistemas de información, aplicaciones, bases de datos, equipos de mitigación de amenazas, hasta la educación en seguridad informática a su personal (González Pérez, 2014).

1.3 Análisis Forense

El Análisis Forense marca una gran diferencia entre los demás conceptos relacionados con Seguridad Informática, debido a que este no busca evaluar o encontrar fallos de seguridad en una organización o empresa, sino que intenta demostrar una serie de sucesos en un escenario específico; es decir, un analizador forense mediante técnicas de recopilación y peritaje de datos, puede recuperar y tratar la información después de que un incidente de seguridad haya ocurrido, por ejemplo: corromper las políticas de seguridad de un sistema, para lo cual el analizador forense tratará de deducir la naturaleza del ataque (González Pérez, Sánchez Garcés, & Soriano de la Cámara, 2015).

En conclusión, el análisis forense de cualquier tipo tiene como objetivo principal contestar tres preguntas esenciales al momento de aclarar un incidente de seguridad:

Ilustración 1.2 Interrogantes principales solventadas por el análisis forense.
Fuente: Pentesting con Kali 2.0, pág. 21.

El proceso de un análisis forense requiere una serie de herramientas especializadas, por lo tanto, Kali es la distribución de Linux por excelencia para esta tarea, ya que además de contar con una completa gama de herramientas, también cuenta con el Modo Forense,

importantísimo para evitar la pérdida de evidencias (González Pérez, Sánchez Garcés, & Soriano de la Cámara, 2015).

Las características principales que permite el Modo Forense en Kali son las siguientes:

- Los discos duros internos no serán utilizados, ni montados automáticamente incluyendo la partición “swap” o intercambio.
- El soporte automático de cualquier medio externo esta desactivado, es decir, si un disco compacto, una unidad USB o un disco duro externo es insertado en el equipo, Kali no lo montará automáticamente, sino que esperará a que el usuario bajo su responsabilidad de la orden de ejecutar esta acción.

Ilustración 1.3 Inicio a modo forense en Kali Linux.
Fuente: http://docs.kali.org/general-use/kali-linux-forensics-mode

1.4 Hacker

Un hacker es una persona con conocimientos profundos en diversas ramas relacionadas a la informática, el cual es capaz de encontrar fallos de seguridad, reportarlos y corregirlos; protegiendo así los activos tecnológicos de una empresa. Además, se lo puede definir como un investigador con la habilidad de superar los límites de alguna tecnología que sus propios creadores impusieron.

A menudo se suele confundir un hacker con un cibercriminal o cracker, pero lo cierto es que un hacker no utiliza sus conocimientos para dañar ningún activo tecnológico, es decir, un hacker construye cosas mientras que un cracker las destruye (Raymond, 2015).

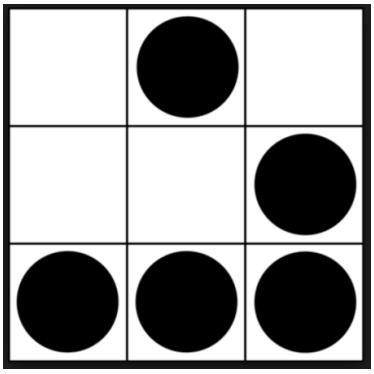


Ilustración 1.4 The Glider - Emblema universal de la cultura hacker.
Fuente: http://www.catb.org/hacker-emblem/

1.4.1 Tipos de hacker

Existen varios términos para las personas en el mundo de la seguridad informática, pero los tres tipos de hackers a continuación son los que más sobresalen:

a) White hats o sombreros blancos

Son personas que utilizan sus conocimientos con fines beneficiosos y éticos, se encargan de proteger los activos tecnológicos de una empresa asegurando la integridad, disponibilidad y confidencialidad de la información. Se considera a los White hats como hackers éticos (González Pérez, 2014).

b) Black hats o sombreros negros

Son personas que usan sus conocimientos en informática con fines maliciosos o solo para su beneficio personal. Son también considerados crackers o cibercriminales, los cuales cometen actividades ilegales con repercusiones jurídicas muy graves. Los hackers de sobrero negro se caracterizan por realizar ataques con un impacto negativo muy fuerte para la organización, por ejemplo: denegación de servicios, violación de sistemas de seguridad, intrusión a zonas privadas sin autorización, secuestro de información e infección de redes (González Pérez, 2014).

c) Grey hats o sombreros grises

Es un híbrido entre White y Black hats, son personas que utilizan sus conocimientos de informática para irrumpir en sistemas o adquirir información simplemente por curiosidad o para demostrar sus conocimientos, pero en la mayoría de los casos, aunque actúe ilegalmente, no tiene como objetivo principal destruir (González Pérez, 2014).

Además, cabe destacar varios términos adicionales muy utilizados para clasificar personas dentro del mundo del Hacking:

Samurai: son personas contratadas por empresas para investigar y encontrar fallos de seguridad, su especialidad es investigar casos sobre los derechos de privacidad, se oponen completamente a los crackers o cibercriminales.

Phreaker: son personas con avanzados conocimientos en telefonía modular, tecnologías de telecomunicaciones, dispositivos móviles, que podrían llegar a realizar acciones no autorizadas.

Wannabe: se define a las personas interesadas por el fascinante mundo del hacking ético y las cuales se encuentren estudiándolo.

Lammer: se atribuye este término a personas que presumen conocimientos y habilidades de hacking que en realidad no poseen, es decir aparentan ser hackers, pero no lo son. Este tipo de personas también llamadas script-kiddie buscan aplicaciones y herramientas de hacking para ejecutarlas sin entender su funcionamiento e ignorando las consecuencias que esto podría conllevar.

Carder: es una persona dedicada a clonar, utilizar o realizar cualquier otra actividad fraudulenta relacionada con tarjetas de crédito que no son de su propiedad.

Newbie: son personas novatas en el mundo de la seguridad informática, los cuales no disponen de mucho conocimiento sobre esta.

1.5 Tipos de auditoría

Existen varios tipos de auditorías base en un proceso de Hacking Ético, algunas de ellas pueden dividirse en auditorías más específicas, como se indica en la siguiente ilustración:

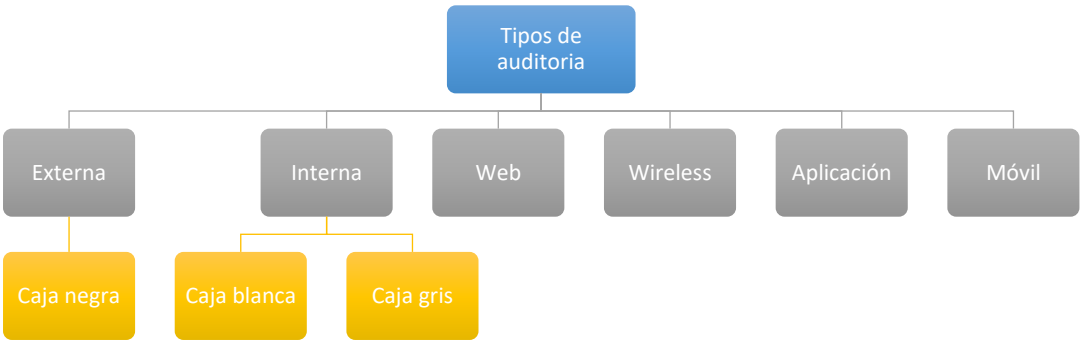


Ilustración 1.5 Tipos de auditorías.
Fuente: Pentesting con Kali 2.0, pág.18 a 20.

1.5.1 Auditoría Externa

También conocida como ***auditoría de caja negra***, en esta el auditor simula un ataque muy parecido al que sería realizado por un cibercriminal real, sin accesos o conocimientos previos sobre la empresa objetivo. El auditor comenzará realizando una investigación y recopilación de información pública referente a su objetivo, para después asociarla con los servicios y sistemas públicos con los que la empresa a evaluar cuente.

Existen dos fases primordiales en una auditoría externa denominadas:

a) **Footprinting:** es la exploración y recopilación de información pública del objetivo.
b) **Fingerprinting:** con la información antes obtenida se realiza la enumeración e interacción con los servicios y sistemas públicos del objetivo.

El objetivo de este tipo de auditoría es evaluar la seguridad de una empresa mediante un ataque externo simulado, y de esta forma encontrar el mayor número de posibles vulnerabilidades presentes en servicios tecnológicos públicos, relacionados directa o indirectamente con la empresa evaluada. Este tipo de auditoría es una de las más costosas debido a que toma más tiempo realizarla (González Pérez, Sánchez Garcés, & Soriano de la Cámara, 2015).

1.5.2 Auditoría Interna

En esta el auditor poseerá ciertos permisos, información y privilegios de la empresa a evaluar, y de acuerdo con estos se podrá determinar si la auditoría es de caja blanca o de caja gris.

a) **Auditoría de caja blanca:** el auditor asume el rol de un usuario interno de la organización el cual cuenta con privilegios especiales en los sistemas internos y acceso a la información crítica total o parcial de la organización. Generalmente este tipo de auditoria es realizada por el personal de seguridad informática de la organización, o un pentester contratado por dicha empresa, el cual trabajará en conjunto con el departamento de tecnología interno. Es de vital importancia realizar este tipo de auditorías constantemente, ya que muchas empresas creen que sus sistemas no presentan vulnerabilidades y descuidan su seguridad informática, por lo tanto, esta investigación permite identificar los puntos débiles en la plataforma tecnológica organizacional y además comprobar lo que un usuario con ciertos permisos puede llegar a lograr (González Pérez, 2014).

Los aspectos fundamentales por revisar en este tipo de auditoría son:

- Políticas que se relacionen directa o indirectamente con la plataforma tecnológica empresarial.
- Servicios tecnológicos.
- Redes empresariales.
- Código de aplicativos utilizados en la organización.
- Software implementado.
- Configuraciones de equipos informáticos.
- Educación en seguridad informática al personal en general.

b) Auditoría de caja gris: es un tipo de auditoría híbrida entre la de caja blanca y caja negra, ya que el auditor toma el rol de un cliente o empleado interno de la organización con pocos o ningún privilegio sobre la plataforma tecnológica empresarial. El auditor no cuenta con el mismo nivel de acceso e información que en la de caja blanca, por lo tanto, se le facilita información básica sobre la plataforma tecnológica organizativa, con el objetivo de intentar obtener mayores privilegios y acceder a información confidencial a la que no tiene acceso, simulando un ataque interno a la organización. Es muy común iniciar esta auditoría ingresando a la red interna a través del acceso inalámbrico (Wi-Fi) o una terminal de un empleado (González Pérez, 2014).

1.5.3 Auditoría Web

Este tipo de auditoría es muy popular dentro del mundo de la seguridad informática, debido a que las empresas siempre han tenido una gran preocupación sobre las vulnerabilidades que un sitio web expuesto a internet puede presentar, por lo tanto, actualmente las organizaciones toman mayores medidas de seguridad para controlar sus sistemas web, como por ejemplo la utilización de frameworks y gestores de contenido (González Pérez, Sánchez Garcés, & Soriano de la Cámara, 2015).

Un sitio web independientemente de la herramienta o tecnología utilizada puede presentar vulnerabilidades debido a: falla en el diseño o implementación del sistema web, desarrollo de software descuidado sin estándares, control de acceso inadecuado y sin protección (González Pérez, Sánchez Garcés, & Soriano de la Cámara, 2015).

Ilustración 1.6 Auditoría de Seguridad Web.
Fuente: Pentesting con Kali 2.0, pág. 20.

1.5.4 Auditoría Wireless

Se la relaciona con la auditoría interna, sin embargo, debido al gran número de aspectos a considerar cuando se la realiza, es necesario estudiarla a detalle e independientemente de las auditorias antes mencionadas. En esta, el auditor se enfoca principalmente a verificar varios aspectos relacionados con la red inalámbrica de una organización como: intensidad de la señal, interferencias, descubrimiento de puntos de acceso, configuraciones adecuadas de los puntos de acceso, protocolos, cifrado de conectividad inalámbrica y monitoreo permanente de la red inalámbrica (González Pérez, Sánchez Garcés, & Soriano de la Cámara, 2015).

La suite de herramientas más conocida para realizar este tipo de auditoría es *Aircrack,* la cual encontramos de manera nativa en la distribución de Linux, Kali. Adicionalmente, la metodología más recomendable a utilizarse es la OWISAM (Open Wireless Security Assessment Methodology), la cual indica al auditor los controles de seguridad más comunes a ser verificados en las redes inalámbricas (González Pérez, Sánchez Garcés, & Soriano de la Cámara, 2015).

1.5.5 Auditoría de Aplicación

Este tipo de auditoría tiene por objetivo evaluar la integridad de una aplicación, para conocer si esta presenta errores o vulnerabilidades de seguridad. Las fases secuenciales recomendadas para realizar esta auditoría son:

a) Realizar un análisis funcional del aplicativo.
b) Efectuar un análisis técnico del aplicativo.
c) Diseñar las pruebas a utilizar.
d) Desarrollar las pruebas diseñadas.
e) Ejecutar las pruebas preparadas.

1.5.6 Auditoría Móvil

Se enfoca en el análisis de un dispositivo o grupo de dispositivos móviles en una organización, por lo general es necesario disponer de permisos de super usuario en el equipo, por lo tanto, si el dispositivo cuenta con el sistema operativo iOS de Apple, será necesario realizar un jailbreak; y si el dispositivo cuenta con el sistema operativo Android de Google, será necesario realizar un rooting.

1.6 Software malicioso (Malware)

El software malicioso o más conocido como Malware; se define como todo código o software desarrollado con fines dañinos y destructivos, los cuales atentan contra la integridad, confidencialidad y disponibilidad de equipos informáticos, redes, sistemas o información. Todo tipo de software malicioso es creado a partir de una vulnerabilidad explotada por un cibercriminal (CISCO Systems, 2015).

Según (CISCO Systems, 2015) el malware tiene varias formas de infectar sistemas y propagarse, como, por ejemplo:

a) Ocultando su código en otros programas o adjuntándose como macros en los archivos.
b) Explotando vulnerabilidades en el sistema operativo, dispositivo de red u otro software.
c) Aprovechando huecos de seguridad en los navegadores web por medio de visitas a páginas web corruptas.
d) Escondiéndose en archivos adjuntos de correo electrónico o descargados de internet.

En el caso de este último generalmente las acciones para que se produzca una infección son realizadas por el usuario, el cual, por desconocimiento o malicia, ejecuta o descarga archivos de origen desconocido o inseguro.

El malware se encuentra en constante crecimiento y evolución; volviéndose más complejo de detectar y consecuentemente más rentable para quienes lo usan con fines maliciosos. Según (Ponemon Institute, 2014) se calcula que más de 300.000 nuevos archivos maliciosos son creados cada día y liberados en internet, el impacto económico de una brecha de seguridad informática en una organización es de alrededor $3,5 millones por año, con un incremento anual del 15% aproximadamente. Adicionalmente, cabe destacar que la mayor amenaza dentro de una organización son los empleados sin educación o concientización en seguridad informática, ya que podrían ejecutar códigos maliciosos, generando un vector de ataque potencial para un cibercriminal.

1.6.1 Clasificación del software malicioso

Generalmente se ha catalogado a todo software malicioso como “virus”, pero en realidad este es solo una pequeña parte de un gran abanico de tipos de malware, de hecho, las variantes de este van desde amenazas leves como molestos anuncios publicitarios, hasta amenazas críticas como robo de información confidencial o cuentas bancarias, destrucción de información e inhabilitación de equipos informáticos o redes (CISCO Systems, 2015).

Las variantes de malware se diferencian, de acuerdo con las formas de infección y propagación que utilizan; por lo tanto, se las puede clasificar como se muestra a continuación:

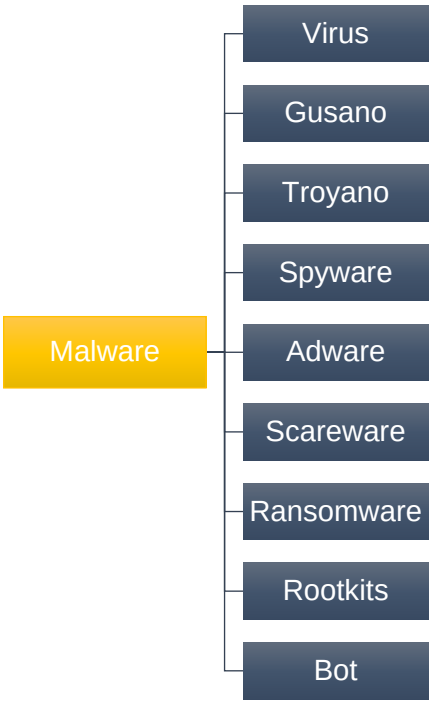


Ilustración 1.7 Tipos de amenazas informáticas.
Fuente: Propia.

a) Virus

Este tipo de malware se propaga mediante otro programa externo en el cual se aloja, tiene por objetivo alterar el funcionamiento normal de un equipo computacional y necesariamente el usuario tiene que ejecutarlo para que se active, es decir cuando el usuario inicie el código del programa original, también ejecutará el código del virus; generalmente no afectan al software en donde se alojan, sin embargo, en ocasiones pueden sobrescribirlo con copias de si mismos, o inclusive difundirse a través de la red (CISCO Systems, 2015).

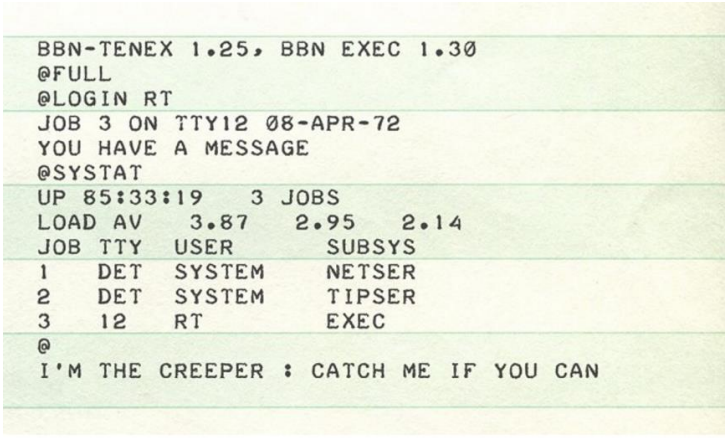


Ilustración 1.8 Código de “Creeper”, el primer virus informático creado.
Fuente: https://www.xataka.com/historia-tecnologica/la-historia-de-creeper-el-primer-virus-informatico-jamas-programado

b) Gusano

Son muy similares a los virus ya que replican copias de sí mismos y el daño que causan es muy parecido. La diferencia de los gusanos frente a los virus es que estos no necesitan de un programa o archivo donde alojarse o de acciones del usuario para propagarse, sino lo realiza mediante la explotación de vulnerabilidades en los sistemas objetivos. Una vez que el gusano haya ingresado a un equipo computacional, este toma control sobre las características de transporte de archivos o información para poder replicarse a través de la red (CISCO Systems, 2015).

c) Troyano

Este tipo de malware hace referencia al caballo de Troya en la mitología griega, y tiene por objetivo engañar al usuario haciéndose pasar por software legítimo, para que este lo ejecute en sus sistemas. Los ataques de los troyanos son muy variados y van desde la visualización no consentida de publicidad molesta al usuario hasta la destrucción de información crítica del usuario. Además, pueden complementar sus ataques con la ejecución de otros tipos de malware como virus o adware, y también son capaces de crear puertas traseras (back doors) en los sistemas informáticos para asegurar la mantenencia del acceso no autorizado a los mismos (CISCO Systems, 2015).

Los troyanos no son capaces de propagarse por si mismos como los virus o gusanos, por lo que necesitan de la acción del usuario para conseguirlo, las vías de infección típicas son a través de adjuntos de correo electrónico o descargas de archivos desde internet (CISCO Systems, 2015).

La variante más peligrosa es conocida como Remote Access Trojan (RAT) la cual permite tomar el control remoto total del equipo infectado, pudiendo robar información confidencial y además atentando en contra de la privacidad de la víctima.

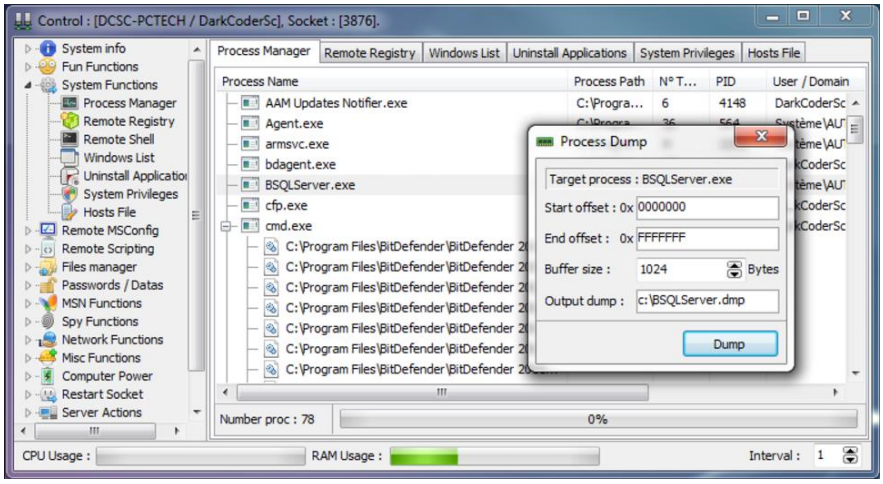


Ilustración 1.9 Remote Access Trojan (RAT) en funcionamiento.
Fuente: https://blog.malwarebytes.com/threats/remote-access-trojan-rat/

d) Spyware

Se dedican a espiar y recopilar información de una persona u organización sin su permiso o conocimiento, para posteriormente utilizar los datos robados en publicidad (minería de datos), extorciones o cualquier acción ilegal que beneficie económicamente al cibercriminal espía.

Generalmente este tipo de malware se propaga mediante las descargas de software gratuito de sitios web o redes P2P, la instalación de un spyware es completamente silenciosa, encubriéndose con la ejecución de otro software diferente. En la mayoría de programas gratuitos (freeware) se puede encontrar una clausula en los términos y condiciones, la cual advierte al usuario que su información puede ser recolectada para diferentes fines, ya sean maliciosos, comerciales o para la mejora del software (Panda Security, 2017).

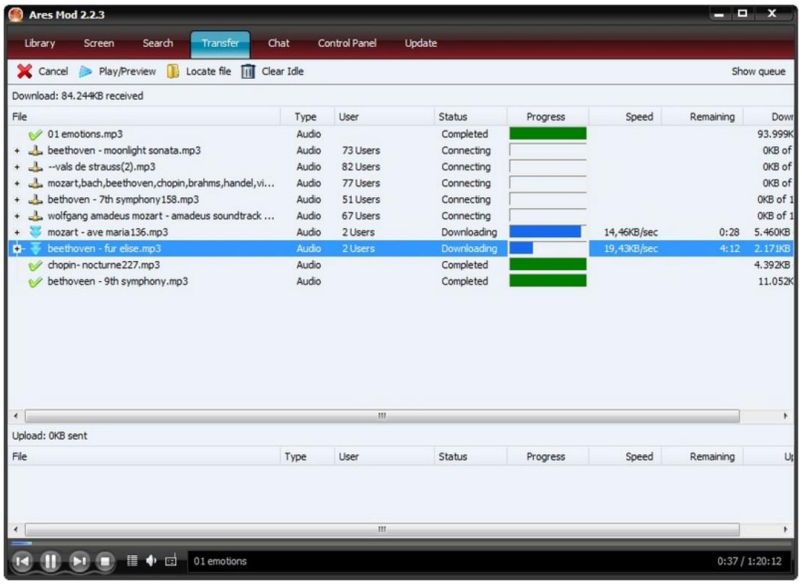


Ilustración 1.10 Ares, cliente de red P2P.
Fuente: https://sourceforge.net/projects/aresgalaxy/

e) Adware

Este malware es mayormente como software publicitario, ya que su único objetivo es llenar el dispositivo infectado con publicidad mediante una gran cantidad de ventanas emergentes o barras de herramientas llenas de publicidad “toolbars”. Generalmente, el adware solo se dedica a mostrar publicidad molesta, pero existen variantes con la capacidad de robar información, monitorizar los hábitos de navegación web o inclusive registrar las pulsaciones del teclado que se realicen. Se encuentran presentes en software gratuito “freeware” (AVAST Software s.r.o., 2015).

Ilustración 1.11 Toolbars de publicidad instaladas en Internet Explorer.
Fuente: http://www.pandasecurity.com/mediacenter/tips/next-next-next/

f) Ransomware

También conocido como scareware, es el tipo de software malicioso más peligroso en la actualidad, ya que tiene por objetivo principal engañar al usuario para que lo descargue haciéndose pasar por software legítimo, adjunto de correo electrónico, o mediante navegación web, el cual una vez descargado se ejecuta y cifra los archivos más importantes del equipo mediante procedimientos criptográficos, y posteriormente demandar un pago de rescate para descifrarlos a la normalidad (Cluley, 2014).

La mejor manera de protegerse contra el ransomware es comprobar que se encuentren instaladas las últimas actualizaciones del sistema operativo y aplicaciones adicionales utilizadas, contar con un producto integral de seguridad informática, evitar divulgar la dirección de correo electrónico, revisar el remitente y adjuntos de correos electrónicos recibidos, educar al personal de la organización en seguridad informática y finalmente contar con una política de respaldos adecuada (Cluley, 2014).

Ilustración 1.12 Ventana principal del ransoware Wannacry 2,0.
Fuente: http://www.elladodelmal.com/2017/05/el-ataque-del-ransomware-wannacry.html

El ciclo de operación de un ransomware ha sido resumido en la siguiente ilustración:

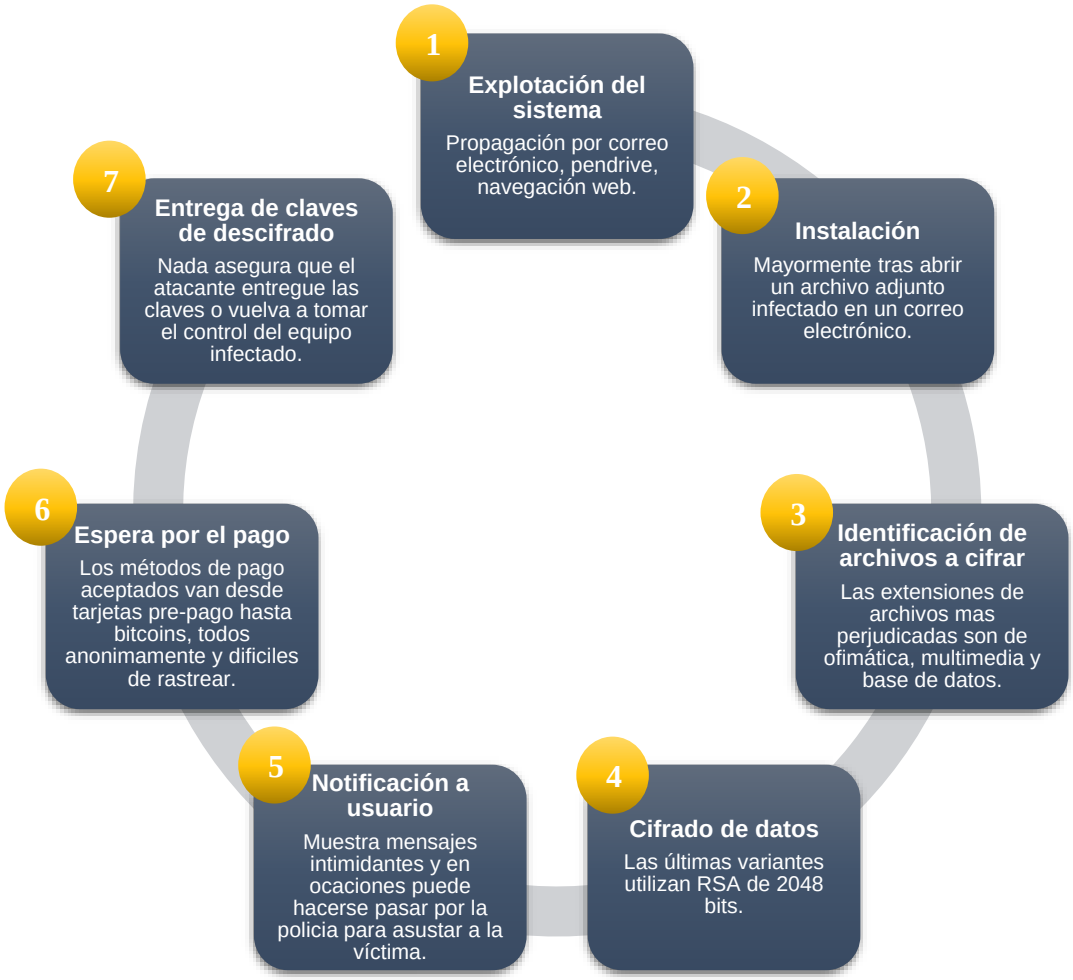


Ilustración 1.13 Ciclo de funcionamiento del ransomware.
Fuente: https://www.welivesecurity.com/la-es/2014/06/10/todo-sobre-ransomware-guia-basica-preguntas-frecuentes/

Anteriormente este tipo de malware no era tan peligroso ya que simplemente mostraba mensajes falsos sobre un gran número de “virus” encontrados, y la única manera de eliminarlos era comprando la versión completa de este supuesto “antivirus”, de manera evidente no era más que un código malicioso de intimidación y estafa, que en muchos casos no se lo podía desinstalar o cerrar para utilizar con normalidad el equipo, hasta que se pague la cantidad demandada o sea exterminado con una solución de seguridad.

Ilustración 1.14 Scareware, Internet Security 2010 mostrando mensajes intimidantes.
Fuente: http://www.malwarehelp.org/internet-security-2010-removal-2010.html

g) Rootkits

Son herramientas utilizadas por los cibercriminales para conseguir y mantener el acceso administrativo a un equipo o sistema informático sin el conocimiento del usuario propietario. Por lo general este tipo de código malicioso encubre sus procesos de ejecución, archivos y datos haciéndolo muy difícil de detectar. Un equipo infectado con rootkits se lo conoce comúnmente como rooteado (AVAST Software s.r.o., 2015).

Existen tres tipos de rootkits, los cuales serán descritos a continuación:

- **Kernel Rootkits:** ocultan una puerta trasera en los sistemas computacionales de un equipo mediante el uso de un código modificado para añadir o reemplazar una porción del código existente del núcleo (kernel) del sistema, generalmente son los rootkits más peligrosos y difíciles de detectar.
- **Library Rootkits:** esconden la información sobre la intrusión por medio de la manipulación de las llamadas del sistema utilizando parches, hooks o reemplazos de código.
- **Application Rootkits:** modifican o reemplazan la información binaria de una aplicación regular mediante parches, inyección de código y hacks.

h) Bot

Su nombre proviene de la palabra “robot” y se lo puede definir como un proceso automático dedicado a interactuar con varios servicios de red. Su objetivo principal es automatizar tareas y proveer servicios o información, los cuales habitualmente serian realizados por un humano. En el mundo del cibercrimen, los bots son utilizados con fines maliciosos, los cuales son capaces de auto propagarse infectando a una gran cantidad de equipos informáticos, los mismos que posteriormente se reportarán a un servidor o servidores centralizados (C&C) que actuarán como centro de control para la red completa de equipos zombie a su mando, más conocida como “botnet” (CISCO Systems, 2015).

En una botnet el equipo comprometido es conocido como “zombie”, mientras que la persona encargada de dar órdenes y dueña de los bots se llama “bot herder”. Mediante una botnet los atacantes son capaces de:

- Tomar control remoto total o parcial del equipo infectado.
- Realizar ataques de denegación de servicio (DoS).
- Adquisición de las pulsaciones de teclas en el equipo infectado (log keystrokes).
- Obtención de contraseñas.
- Captura y análisis de paquetes enviados a través de la red.
- Adquisición de información financiera.
- Reenviar spam.
- Abrir puertas traseras en los equipos infectados.
- Descargar y ejecutar malware adicional en su objetivo.

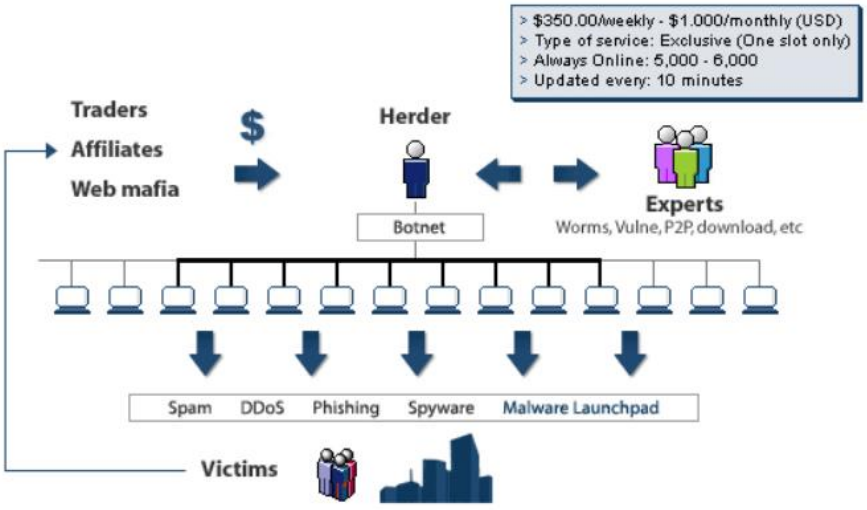


Ilustración 1.15 Ilustración de la operación de una Botnet.
Fuente: http://www.pandasecurity.com/homeusers/security-info/cybercrime/others/

1.7 Vulnerabilidades

El proceso de auditoría ética tiene por objetivo principal evaluar la seguridad tecnológica en una organización, descubriendo los fallos que esta podría tener, para posteriormente recomendar procedimientos de control y contramedida necesarios en la corrección de los mismos. Por lo tanto, se puede definir a una vulnerabilidad como el punto débil de un software, hardware, usuario (ingeniería social) o procedimiento que permita a un cibercriminal llevar a cabo acciones ilegales y no autorizadas en contra de un usuario u organización (González Pérez, 2014).

No todas son iguales, unas atentan directamente en contra de los activos de la organización suponiendo pérdidas económicas graves; mientras que otras con el mismo nivel de importancia, involucran a los activos de la empresa indirectamente. También, existen vulnerabilidades netamente informativas, las mismas que pueden proporcionar datos confidenciales al cibercriminal, atentando en contra de la privacidad del usuario u organización.

Por lo tanto, en un proceso de auditoría las vulnerabilidades pueden ser caracterizadas en base a su estado y riesgo según las siguientes tablas:

Tabla 1.1
Clasificación de estados de vulnerabilidades

ESTADO	
✓	Realizado
✗	No Aplicable
	Documentado
	En Ejecución

Fuente: Ethical Hacking teoría y práctica para la realización de un Pentesting, pág. 23

Tabla 1.2
Clasificación de criticidad de vulnerabilidades

RIESGO	
	Correcto
	Baja

	Media
	Grave

Fuente: Ethical Hacking teoría y práctica para la realización de un Pentesting, pág. 23.

Cabe destacar que en un proceso de Ethical Hacking, la identificación y clasificación de una vulnerabilidad debe seguir una serie de estándares que permitan homogeneizarlas; por lo tanto, en una auditoría se pueden utilizar los siguientes estándares de clasificación de vulnerabilidades: CWE (Common Weakness Enumeration), CVE (Common Vulnerabilities Exposures), CVSS (Common Vulnerability Scoring System) (González Pérez, 2014).

1.8 Riesgos críticos en aplicaciones Web

El proyecto OWASP (Open Web Application Security Project) se encarga del mejoramiento de la seguridad de las aplicaciones web, el cual dentro de su plan de iniciativas esta la emisión del proyecto llamado “OWASP Top 10” en donde se indican los diez mayores riesgos de seguridad para aplicaciones web a nivel global (Alonso, 2017).

A continuación, se enlistan y describen cada uno de los riesgos expuestos en el OWASP Top 10 - 2017:

1.8.1 Inyección

Este tipo de fallas se presentan cuando información no verificada e insegura es enviada a un intérprete como parte de una consulta o un comando, encontramos los siguientes: SQL Injetcion, LDAP Injection, XPath Injection y Command Injection (The OWASP Foundation, 2017).

Cabe destacar que la inyección SQL publicada en diciembre del año 1998, actualmente sigue siendo la más utilizada para atacar sistemas informáticos.

1.8.2 Pérdida de Autenticación y Gestión de sesiones

La gestión incorrecta de autentificación de usuarios o de sesiones en las aplicaciones, permiten a los cibercriminales comprometer contraseñas, keys, tokens de sesión, o explotar otras vulnerabilidades relacionadas para asumir identidades de otros usuarios temporal o permanentemente. Generalmente, este problema es causado por aplicaciones que no caducan sus sesiones enviadas por GET y quedan indexadas en buscadores o proxies, o en casos donde la aplicación tiene un método de autentificación de sesión ineficiente. Los

ataques más conocidos son: Pass-the-hash, Session Hijacking y Session Fixation (The OWASP Foundation, 2017).

1.8.3 Secuencia de Comandos en Sitios Cruzados (XSS)

Los ataques de XSS son muy conocidos dentro del mundo del hacking, éstos a menudo ocurren cuando una aplicación envía información sin verificar e insegura a una página web en un navegador, es decir permite a un cibercriminal inyectar o ejecutar código malicioso en páginas web consultadas por su víctima. Las principales repercusiones de este tipo de fallas son: páginas web manipuladas, robo de información (sesiones de usuario, usuarios, contraseñas), destrucción de sitios web y redirecciones a sitios web maliciosos (The OWASP Foundation, 2017).

1.8.4 Control de acceso desprotegido

En muchas aplicaciones web el control de autentificaciones de usuarios, así como sus respectivos roles y restricciones no están aseguradas correctamente; permitiendo a un usuario convencional o un atacante no autenticado acceder a zonas de una aplicación a la cual no tiene permisos. Los objetivos más susceptibles a este tipo de ataques son los servidores de aplicaciones, servidores web y entornos de aplicaciones web (The OWASP Foundation, 2017).

1.8.5 Configuración de seguridad incorrecta

Una de las principales brechas de seguridad en las empresas u organizaciones, es la incorrecta configuración de seguridad en sus equipos informáticos o aplicaciones, como por ejemplo la utilización de contraseñas por defecto o la asignación inadecuada de los privilegios de un usuario. Por lo tanto, es de vital importancia contar con una configuración de seguridad bien definida e implementada en las aplicaciones, equipos, frameworks y servidores. Además, cabe destacar que dentro de una política de configuración de seguridad adecuada debe exigirse que todo el software se mantenga actualizado, y de esta forma evitar ataques ya conocidos (The OWASP Foundation, 2017).

1.8.6 Exposición de datos sensibles

La mayoría de aplicaciones web no cuentan con métodos de protección adecuados para el manejo y almacenamiento de datos críticos (datos financieros, médicos), por lo que estos pueden ser fácilmente robados, modificados o borrados por atacantes, con el objetivo de efectuar fraudes, robos de identidad o extorciones. Las aplicaciones que vayan a manejar datos sensibles deben utilizar mecanismos de protección especiales como por ejemplo un cifrado de información robusto o la utilización de un segundo factor de autentificación “2FA” (The OWASP Foundation, 2017).

1.8.7 Protección insuficiente frente a ataques

Generalmente las aplicaciones web, así como también las APIs, no cuentan con la habilidad esencial de detectar, prevenir y responder ataques; por lo tanto, una aplicación web tiene que ir más allá que las típicas validaciones en los formularios de ingreso de datos, y tratar de que sea capaz de detectar, documentar, responder e incluso detener ataques hacia sí misma (The OWASP Foundation, 2017).

La siguiente ilustración muestra algunos de los mecanismos de seguridad recomendados en los diferentes ámbitos a proteger en una aplicación web:

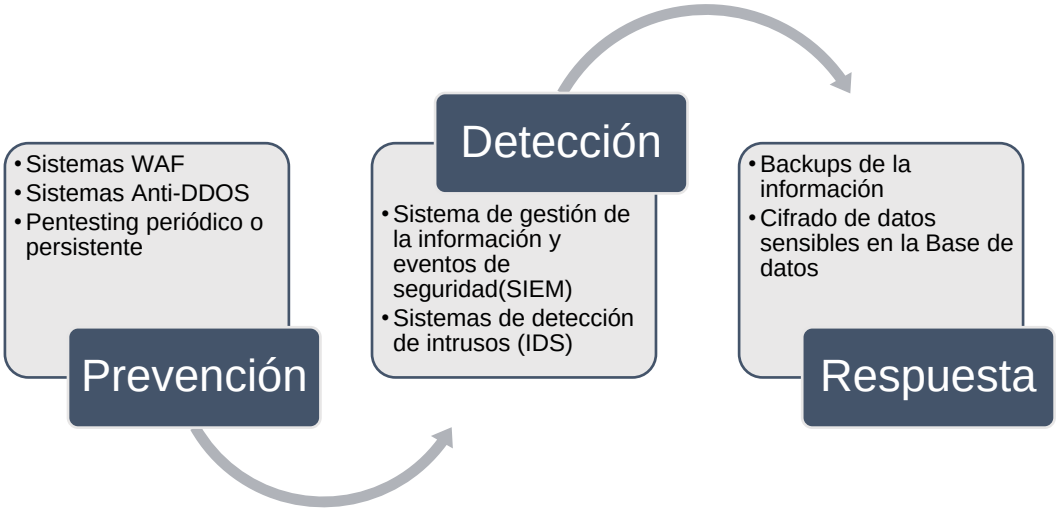


Ilustración 1.16 Mecanismos de protección de aplicaciones web.
Fuente: Blog El lado del mal (http://www.elladodelmal.com/2017/04/publicada-owasp-top-ten-2017-release.html)

1.8.8 Falsificación de Peticiones en Sitios Cruzados (CSRF)

Este tipo de ataques fuerzan al explorador web de un usuario autenticado al envío de peticiones HTTP falsificadas a una aplicación web vulnerable, la cual puede incurrir en el robo de sesiones de usuario (cookies) o cualquier información relacionada con la autentificación del usuario atacado. Las aplicaciones web vulnerables a este tipo de ataques son las que no cuentan con ninguna protección anti-CSRF en sus enlaces internos, por lo tanto, las organizaciones con este fallo pueden sufrir un gran impacto debido a ataques de APTs (Advance Persistent Thereats) como el “Spear-phishing” (The OWASP Foundation, 2017).

1.8.9 Utilización de componentes con vulnerabilidades conocidas

En este apartado se indica el riesgo del uso de herramientas, frameworks, librerías y módulos de software en general que en la mayoría de los casos necesitan obligatoriamente todos los privilegios para funcionar. Por lo tanto, si uno de los componentes vulnerables poseedor de privilegios en la aplicación es atacado, se facilitará la intrusión del cibercriminal en el equipo o inclusive la destrucción de datos. La utilización de componentes vulnerables

conocidos en aplicaciones web disminuye considerablemente la seguridad de esta, ya que aumentan los posibles vectores de ataque utilizados por un cibercriminal (The OWASP Foundation, 2017).

1.8.10 APIs desprotegidas

Las aplicaciones web y móviles actuales utilizan aplicaciones de clientes enriquecidas como JavaScript en el lado del navegador cliente, la cual se conecta a una API como SOAP (XML), REST (JSON), RPC y GWT; las cuales mayormente se encuentran desprotegidas y presentan varias vulnerabilidades (The OWASP Foundation, 2017).

Este tipo de falla se la puede evidenciar mayormente en las Apps Móviles, las cuales pueden presentar back-ends con APIs muy vulnerables y expuestas a amenazas externas.

1.9 Penetration Test

Es un método mediante el cual un hacker ético busca atacar y comprometer de manera controlada un sistema informático, equipo de computación, red o cualquier otro medio tecnológico utilizado en una organización, con el objetivo de identificar y corregir proactivamente las vulnerabilidades encontradas. Es decir, en una prueba de penetración, las técnicas y procedimientos utilizados son iguales o muy similares a las que emplearía un cibercriminal en un ataque real (González Pérez, 2014).

La diferencia entre un pentester y un cibercriminal es la finalidad que persiguen al vulnerar un medio tecnológico. Mientras que el atacante real busca conseguir beneficio económico mediante el robo, destrucción o modificación de información o cualquier medio tecnológico de la empresa; el pentester busca demostrar las vulnerabilidades en dichos medios, y tratar de corregirlas a tiempo para prevenir futuros ataques.

El pentester tiene la responsabilidad y obligatoriedad de reportar todas las fallas o bugs que posea un sistema y que puedan representar un peligro para la organización.

Además, el Pentesting evalúa el nivel de madurez de la empresa auditada, contribuyendo al mejoramiento de políticas relacionadas con la seguridad informática corporativa; por lo tanto, si una empresa piensa que puede prevenir y estar completamente inmune a cualquier ataque su nivel de madurez es muy bajo. Al contrario, las empresas con un mayor nivel de madurez balancean la inversión entre prevenir y detectar (intrusiones, monitorizar, realizar análisis continuos de código y vulnerabilidades). Por último, las empresas con un nivel de madurez muy alto ya piensan en planes de contingencia cuando un incidente de seguridad comprometa su infraestructura tecnológica, ya sea exteriormente (ataque informático) o interiormente (empleado descontento) (Alonso, 2015).

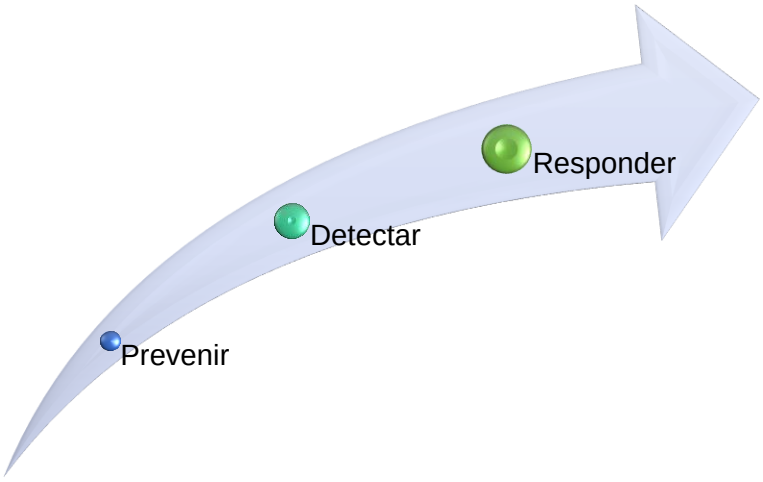


Ilustración 1.17 Nivel de Madurez de una Empresa en Seguridad Informática.
Fuente: Low Hanging Fruit – Chema Alonso (https://www.slideshare.net/chemai64/cybercamp-2015-low-hanging-fruit?ref=http://www.elladodelmal.com/2015/11/do-basics-elimina-el-low-hanging-fruit.html)

1.9.1 Fases del Penetration Test

En un Penetration Test existen etapas diferenciadas, con objetivos específicos distintos y un objetivo final común. El objetivo que comparten todas las fases es realizar el testeo en materia de seguridad dentro de la organización, mientras que los objetivos específicos de cada etapa son aportar información y pruebas sobre el estado de la seguridad informática del objetivo auditado (González Pérez, 2014).

Para realizar un test de penetración es sumamente necesario elegir la metodología que más se ajuste al escenario a auditar, se puede utilizar una metodología establecida o una propia siempre y cuando se mantenga el objetivo principal de un Pentesting. El presente test de penetración de caja blanca será realizado según la metodología desarrollada por la empresa DragonJAR Soluciones y Seguridad Informática S.A.S. la cual fue basada en las siguientes metodologías: a) OSSTMM (Open Source Security Testing Methodology Manual) del instituto para la seguridad y las metodologías abiertas ISECOM, b) Guía de pruebas OWASP (Open Web Application Security Project), que está enfocada a la auditoria de aplicaciones web, c) ISSAF (Information Systems Security Assessment Framework), d) Penetration Testing Framework de Vulnerability Assessment que además de mostrarnos la metodología a seguir, nos sugieren herramientas para realizar cada una de las etapas del Pentest (DragonJAR Soluciones y Seguridad Informática S.A.S., 2015).

En la siguiente ilustración se exponen las fases comprendidas en la metodología usada, y posterior se describen cada una de ellas:

Ilustración 1.18 Diagrama de la metodología a utilizar.
Fuente: https://www.dragonjar.education/leccion/introduccion-al-pentesting-metodologia/

a) Fase de Recolección de Información

Es una de las fases más importantes de la investigación en la cual el pentester debe recoger la mayor cantidad de información sobre la empresa a auditar, para después crear un perfil del objetivo sin interactuar con el mismo; principalmente se debe identificar datos básicos como, por ejemplo: a qué se dedica, cuál es su core de negocio y cómo está conformada la empresa. Esta fase se caracteriza por ser una recopilación de información de una manera pasiva, es decir, no se genera un contacto directo a los activos tecnológicos de la empresa a auditar, sino que regularmente se realizan consultas públicas en internet sobre el objetivo (DragonJAR Soluciones y Seguridad Informática S.A.S., 2015).

Las actividades recomendadas para realizar en esta fase son:

- Hacking con buscadores (Google Hacking).
- Búsqueda de información pública de la empresa empleado la técnica OSINT (Open Source Intelligence o Inteligencia de fuentes abiertas).
- Revisión versiones de la página web en Archive.org.
- Búsqueda inversa de imágenes y logos de la empresa.
- Análisis de DNS, dominio y hospedaje de la página web/correo.
- Reverse IP.

- Extracción y análisis de Metadatos.

b) Fase de Enumeración

Esta etapa del Pentesting es complementaria a la anterior, debido a que se continúa recogiendo información del objetivo, pero ya es posible interactuar directamente con los activos tecnológicos de la organización auditada, es decir ya es posible realizar pruebas intrusivas con herramientas especializadas en Pentesting a los servidores, equipos, sitios web, redes y demás medios tecnológicos pertenecientes a esta. En esta fase se centrará en la identificación activa de los objetivos, mediante escaneos de puertos, identificación de servicios y sistemas operativos (DragonJAR Soluciones y Seguridad Informática S.A.S., 2015).

Las actividades recomendadas para realizar en esta fase son:

- Detección de direcciones IP.
- Detección de equipos activos.
- Detección de DNS (Transferencia de zona).
- Detección de Sistemas operativos.
- Detección de Servicios y sus versiones.
- Detección de IDS, IPS, Firewall, WAFs.

c) Fase de Análisis

En esta etapa ya se tiene contacto directo y en ocasiones agresivo con los activos tecnológicos de la organización, es decir, las pruebas efectuadas ya comprometen directamente a servidores, equipos terminales de usuario, sitios web y redes; causando que sea posible la detección del pentester, por lo cual es de vital importancia tener la autorización y los permisos adecuados por parte de la organización auditada para efectuar los procesos de análisis.

Tiene por objetivo principal utilizar toda la información antes obtenida para ejecutar escáneres de vulnerabilidades y posteriormente exponer las posibles fallas en los medios analizados.

En la presente etapa si algún activo tecnológico auditado ya cuenta con una metodología propia, se la aplica directamente en vez de continuar con la Fase de Explotación del Pentesting (DragonJAR Soluciones y Seguridad Informática S.A.S., 2015).

Las actividades recomendadas a ejecutar son:

- Modelado de la infraestructura, servicios, aplicaciones y sistemas operativos.
- Identificación de fallos conocidos, mediante escáneres de vulnerabilidades.

d) Fase de Explotación

En esta etapa se realizan ataques intrusivos y directos a un objetivo en específico, las técnicas para llevar acabo la explotación son muy diversas pero la más común es la utilización de exploits a través de frameworks (DragonJAR Soluciones y Seguridad Informática S.A.S., 2015).

Las actividades más comunes en esta etapa son:

- Fuerza bruta.
- Cracking Passwords.
- Captura de información de red.
- Ingeniería social.
- Búsqueda y ejecución de exploits conocidos.
- Ataques de DoS.
- Pivoting.
- Escala de privilegios.

e) Fase de Documentación

Una vez completadas las etapas anteriores y a partir de los resultados obtenidos se genera la documentación correspondiente con los detalles que comprendió la auditoría, en los cuales es importante indicar las medidas necesarias a tomar para evitar que la organización sufra ataques e incidentes por parte de cibercriminales reales (DragonJAR Soluciones y Seguridad Informática S.A.S., 2015).

El objetivo principal de esta etapa es exponer a los responsables de la organización auditada todos los resultados logrados, por lo tanto, la documentación generada debe contemplar la explicación del trabajo que se ha realizado en la organización y sobre todo las vulnerabilidades descubiertas en el transcurso del Pentesting. Como mínimo se deben generar dos tipos de informes, como son el ejecutivo y el técnico (González Pérez, 2014).

(González Pérez, 2014) en su obra (Metasploit para Pentesters) afirma lo siguiente:

El informe técnico es un documento con gran nivel de detalle en el que se especifican todas las acciones, con las herramientas, que se han ido utilizando y los resultados que se han ido obteniendo. Además, debe acompañarse de una lista que indique como subsanar esos riesgos y unas recomendaciones del autor (pág. 29).

(González Pérez, 2014) en su obra (Metasploit para Pentesters) afirma lo siguiente:

El informe ejecutivo es un documento más ameno y liviano en el que se deben especificar las vulnerabilidades encontradas, pero sin ningún nivel técnico. Todo debe estar explicado de tal manera que cualquier persona sin capacidades técnicas entienda que riesgos existen en la organización. Además, el propietario de la organización esperará sus recomendaciones como profesional de la seguridad, por lo que en este informe debe existir dicha lista (pág. 29).

1.9.2 Herramientas útiles para realizar un Penetration Test

Foca

Fingerprinting Organizations with Collected Archives (FOCA) es una herramienta orientada principalmente al análisis de metadatos e información oculta de archivos, los mismos que pueden encontrarse en dominios o infraestructuras internas de organizaciones.

Los formatos de archivos que es capaz de analizar son muy variados, siendo los más comunes los de Microsoft Office, Open Office, o PDF, aunque también analiza ficheros de Adobe InDesign, gráficos vectoriales o imágenes de mapa de bits.

Este software se encarga principalmente de la automatización del proceso de búsqueda de servidores usando técnicas enlazadas recursivamente tales como: Web Search, DNS Search, Resolución IP, PTR Scanning, Bing IP, Common names, DNS Prediction y Robtex. En la actualidad es un referente en el ámbito de la seguridad informática, gracias a las numerosas opciones que incorpora, por lo cual es posible realizar múltiples ataques y técnicas de análisis como: extracción de metadatos, análisis de red, DNS Snooping, búsqueda de ficheros comunes, juicy files, búsqueda de proxys, reconocimiento de tecnologías, fingerprinting, leaks, búsqueda de backups, forzado de errores y búsqueda de directorios abiertos (Telefónica Digital España, 2015).

Maltego

Es una herramienta encargada de realizar el proceso de recolección de información de una manera sencilla, rápida y visual. Se basa en entidades, las cuales son objetos sobre los que se aplicaran determinadas acciones que se conocen como transformadas. Estas entidades están divididas en dos categorías: las relacionadas con las infraestructuras y las relacionadas con personas.

Al igual que FOCA, esta es capaz de enlazar información de diversas fuentes y obtener así un mapa de infraestructura que hay detrás de un determinado dominio; además mantiene

una compatibilidad con compañías como Facebook y Twitter (González Pérez, Sánchez Garcés, & Soriano de la Cámara, 2015).

Nessus

Es un escáner de vulnerabilidades disponible en diversos sistemas operativos, es gratuito para su uso personal y entornos no corporativos; tiene una gran cantidad de datos relacionados con las diferentes vulnerabilidades presentes en software comercial, libre y sistemas operativos. Esta herramienta cuenta con tres componentes principales para su funcionamiento: (a) un demonio o componente principal, el cual es el encargado de los chequeos de vulnerabilidades en un host; (b) un cliente que se conecta al servicio o demonio Nessus, mediante el cual se pueden dar directrices o políticas de escaneo de vulnerabilidades, además de permitir la visualización de reportes de escaneos ejecutados anteriormente; (c) Script de Nessus, los cuales son llevados a la práctica en lenguaje de programación NASL (Tenable Inc., 2017).

Características Generales de Nessus:

- Evaluación de vulnerabilidades automatizado.
- Interface de usuario basada en Web.
- Escaneos de vulnerabilidades basado en host y en red.
- Auditoria de Parches.
- Auditoria de Cumplimiento.
- Informes y Reportes.

Wireshark

Se considera uno de los mejores analizadores de tráfico de red y es indispensable al momento de realizar auditorías informáticas en un proceso de Ethical Hacking. Su objetivo principal es mostrar al usuario todo el tráfico que está circulando a través de su interfaz de red. Además, permite elegir por cual interfaz o por cuales se desea llevar a cabo el análisis de tráfico, para después realizar un filtro de los paquetes si es necesario (González Pérez, 2014).

Características principales:

- Se ejecuta en varios sistemas operativos como Windows, macOS o Linux.
- Intercepta y captura paquetes en tiempo real.
- Provee información detallada de los paquetes capturados.

- Soporta importación y exportación de paquetes.
- Cuenta con un control de *sniffing* remoto para capturar paquetes de equipos externos.

Acunetix

Es un escáner de vulnerabilidades orientado a Aplicaciones Web; actualmente solo se ejecuta en Microsoft Windows, pero es capaz de analizar sistemas operativos multiplataforma (Linux, Windows, Solaris). Su objetivo principal es analizar vulnerabilidades orientadas al XSS (Cross-site scripting), SQL Injection, XXE (XML External Entity), SSRF (Server Side Request Forgery) y Host Header Injection (Acunetix, 2017).

Sus principales características son:

- Realiza exploraciones y análisis en profundidad de todos los sitios web objetivo.
- Cuenta con una tasa de detección de vulnerabilidades falsas positivas muy baja.
- Integra un gestor de vulnerabilidades para priorizar y controlar las amenazas encontradas.
- Soporta compatibilidad con WAFs populares y Sistemas de seguimiento de incidentes.
- Ejecuta análisis de seguridad de red y posee herramientas de prueba manual.

Hashcat

Es una aplicación multiplataforma la cual permite recuperar contraseñas a partir del valor del hash para cada una de ellas, es decir toma como entrada un conjunto de palabras en texto plano y calcula el hash para cada una de ellas, comparando contra otro archivo que almacena los hashes de las contraseñas originales; si existen coincidencias las contraseñas serán encontradas. La principal característica de esta herramienta es su capacidad de acelerar notablemente los cálculos mediante la utilización de varios hilos ejecutándose en paralelo. Además, no solo realiza los cálculos utilizando la CPU, sino que también aprovecha el mayor poder de procesamiento de las GPU actuales, pudiendo analizar miles de millones de hashes por segundo (Porolli, 2013).

Nmap

Network mapper o mejor conocido como Nmap es una herramienta multiplataforma, gratuita y de código abierto utilizada para la detección y análisis de redes en una auditoría de seguridad. Utiliza paquetes IP sin procesar para determinar qué hosts están presentes en una

red, qué servicios (nombre y versión) ofrecen, qué sistemas operativos están corriendo y qué tipo de mecanismos de defensa utilizan (Lyon, 2015).

Esta herramienta puede ser utilizada mediante su cliente gráfico Zenmap o por su línea de comandos; la cual generalmente maneja la siguiente sintaxis: "*nmap <tipo de scan> <opciones>".* La ejecución del comando por defecto de nmap es la siguiente: "*nmap <dirección IP>",* misma que retorna información del equipo con dicha dirección IP donde se expone los puertos abiertos, servicios encontrados o el estado de la máquina analizada (González Pérez, 2014).

Metasploit framework

Es un marco de trabajo más conocido como Metasploit, el cual originalmente fue desarrollado en el lenguaje de programación Perl, pero posteriormente fue migrado a lenguaje Ruby. Este framework es un compendio de herramientas con las que el pentester podrá desarrollar y ejecutar exploits, lanzándolos en contra de equipos para comprobar su nivel de seguridad. Además, cuenta con funcionalidades adicionales muy útiles en una auditoría como: el archivo de "shellcodes", herramientas para recolectar información y escáner de vulnerabilidades (González Pérez, 2014).

Este framework está compuesto por módulos, lo cual aumenta considerablemente sus funcionalidades al momento de llevar a cabo una auditoría. Según (González Pérez, Metasploit para Pentesters, 2014): "Un módulo es una pieza o bloque de código que implementa una o varias funcionalidades, como puede ser la ejecución de un *exploit* concreto o la realización de un escaneo sobre máquinas remotas" (pág. 17).

Además, los módulos de este framework componen el corazón de Metasploit y gracias a ellos es tan poderoso. Cabe destacar que estos pueden ser desarrollados por usuarios que necesiten crear funcionalidades personalizadas para su necesidad (González Pérez, 2014).

1.10 Distribuciones Linux más utilizadas en SI

Generalmente, cuando se realizan trabajos relacionados a seguridad informática las opciones por excelencia en cuanto a sistema operativo se refieren, serán las diferentes distribuciones Linux enfocadas a este campo, sin embargo, en Microsoft Windows también encontramos varias buenas herramientas para realizar una auditoría. En este caso, se analizarán las distros de Linux más utilizadas en seguridad informática.

Kali: es la distribución de Linux preferida por ethical hackers al momento de realizar auditorías, está basada en Debian y fue creada por el equipo de Offensive Security para reemplazar a BackTrack; Kali contiene un amplio abanico de herramientas para la realización de un Pentesting o auditoría, entre las funcionalidades de Kali destacan las enfocadas a seguridad informática como el gathering, la explotación, el reversing y el análisis forense (González Pérez, Sánchez Garcés, & Soriano de la Cámara, 2015).

BlackArch Linux: es una distribución derivada de Arch-Linux, con un alto grado de rendimiento debido a que es muy simple, minimalista y liviana, cuenta con alrededor de 1800 herramientas actualizables desde sus repositorios oficiales (Paus, 2016).

BackBox Linux: esta distribución basada en Ubuntu se encuentra en constante actualización por parte de sus desarrolladores, a mediados del año 2017 fue liberada su versión BackBox Linux 5, la cual contiene más de 70 herramientas enfocadas al penetration test y al aseguramiento de la seguridad informática (Paus, 2016).

Pentoo: esta distribución de Linux se encuentra basada en Gentoo Linux, la misma que se encuentra en arquitecturas de 32 y 64 bits. Fue desarrollado por Pentoo Team y está diseñado para consumir la mínima cantidad de recursos posible; se puede ejecutarlo en modo Live o instalarlo en el disco duro. Las aplicaciones preinstaladas son suficientes para llevar acabo un Pentesting de manera eficiente (Paus, 2016).

CAPÍTULO 2

Desarrollo del Test de Intrusión o Pentesting

En este capítulo se desarrollan cada una de las fases que comprende el Pentesting, mismas que han sido basadas en la metodología creada por la empresa DragonJAR Soluciones y Seguridad Informática S.A.S., este trabajo es realizado en la Unión de Cooperativas de Ahorro y Crédito del Norte (UCACNOR), organización en la cual se ha conseguido los permisos necesarios y el consentimiento por parte de las autoridades administrativas. Los responsables encargados por parte de la organización son: Gerente y Coordinador de la Unidad de Tecnologías de la Información y Comunicación (TICs); y los servicios tecnológicos autorizados para el Pentesting son: servidor local, Access point, terminales de usuario y sitio web (con limitante de evitar pruebas agresivas).

Las etapas que se ejecutan en este capítulo consisten en una serie de pruebas específicas denominadas “Pruebas de concepto (PoC)”, destinadas a evaluar un aspecto determinado de la organización. Además, todas las fases son secuenciales, por lo tanto, es estrictamente necesario que se desarrollen en el siguiente orden:

Ilustración 2.1 Orden de ejecución de las fases del Pentesting.
Fuente: Propia.

2.1 Fase de Recolección de Información

Se inicia con la búsqueda y recolección pasiva de información pública acerca de UCACNOR; principalmente se identifican datos básicos de la organización como: a qué se dedica, cuál es su core de negocio y cómo está conformada. No se interactuó directamente con los activos tecnológicos del objetivo, por lo tanto, en esta etapa no se corre el riesgo de detecciones.

Las actividades efectuadas en esta etapa fueron:

- Búsqueda de información pública de la empresa empleado la técnica OSINT (Open Source Intelligence o Inteligencia de fuentes abiertas).
- Revisión de versiones de la página web en Archive.org.
- Búsqueda de direcciones de correo electrónico expuestos.
- Análisis de DNS, dominio y hospedaje de la página web y correo.
- Extracción y análisis de Metadatos.

2.1.1 PoC: Búsqueda de información relevante en página web

El presente trabajo se define como una auditoría de caja blanca por lo tanto el cliente facilitó la dirección URL de su página web “www.ucacnor.org”, misma que al navegar se encontró información relevante acerca de la organización, por lo tanto, se define lo siguiente:

La Unión de Cooperativas de Ahorro y Crédito del Norte (UCACNOR) es un organismo integrador sin fines de lucro de Cooperativas de ahorro y crédito en la Zona 1 de la República del Ecuador; sus actividades principales incluyen: la representación a sus siete Cooperativas Asociadas, la capacitación y desarrollo de proyectos dirigidos a Cooperativas socias y afines a UCACNOR, la utilización de red cooperativista por aseguradoras externas, y alianzas estratégicas con proveedores de productos y servicios tecnológicos. Además, mediante su página web se ha podido adquirir información sobre su ubicación física, el personal de UCACNOR, y su estructura organizacional.

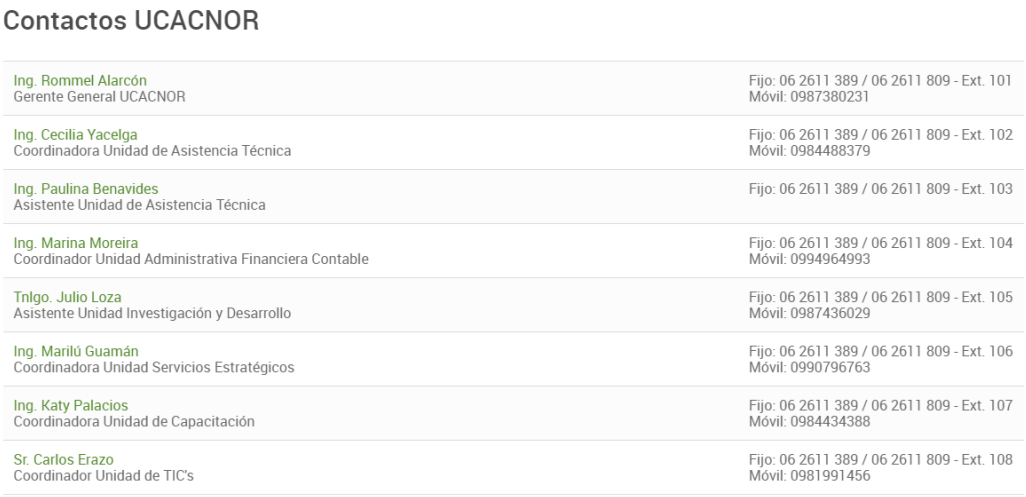


Ilustración 2.2 Lista empleados mostrados en sitio web.
Fuente: Propia

La información encontrada incluye datos que nos servirán para explotarlos en próximas etapas, así como también explorar nuevos vectores de ataque al objetivo. En cada empleado se expone la siguiente información:

Ilustración 2.3 Datos sobre empleado mostrados en sitio web.
Fuente: Propia.

En la ilustración anterior se obtiene fácilmente la dirección de correo electrónico de cada uno de los empleados que conforman la empresa objetivo, esto abre un gran abanico de posibles vectores de ataque como ingeniería social, phising o envío de malware vía correo electrónico, además en la parte inferior existe un botón llamado “Formulario de contacto”, el cual al presionarlo despliega un formulario para realizar envíos al correo del empleado directamente; esto puede significar una potencial amenaza, ya que no se controla la identidad, ni el contenido enviado por correo.

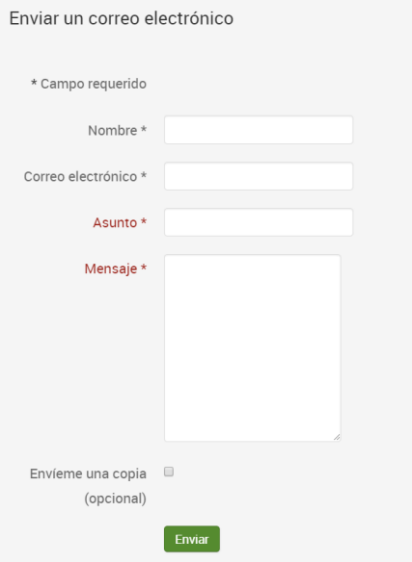


Ilustración 2.4 Formulario de envío de correo electrónico a empleados.
Fuente: Propia.

Otro aspecto fundamental en la recolección de información en la página web de UCACNOR es el análisis del fichero “robots.txt”, el cual en la mayoría de casos es encontrado en la raíz del directorio del sitio web y muchas de las veces provee información valiosa para el Pentesting e inclusive podría llegar a dirigirlo (Rando, González, Aparicio, Martín, & Alonso, 2016).

Para verificar el directorio raíz del sitio web se ingresó la siguiente URL en el navegador: “www.ucacnor.org/web/” y posteriormente se buscó el fichero “robots.txt”:

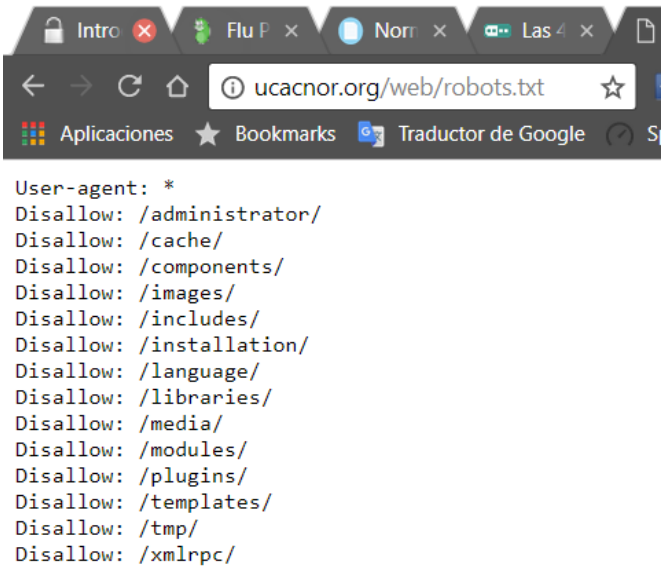


Ilustración 2.5 Fichero “robots.txt” en sitio web auditado.
Fuente: Propia.

El archivo analizado anteriormente expone directorios deshabilitados pero existentes en el sitio web, por lo tanto, un cibercriminal podría tratar de acceder a ellos conociendo su nombre; es muy recomendable que se elimine la información mostrada por este archivo.

Finalmente, en el proceso de recolección de información, se encontró una evidencia que da grandes indicios para afirmar que el sitio web ha sido comprometido anteriormente, lo cual puede significar una potencial amenaza en contra de la privacidad, veracidad e integridad de los datos del sitio web, debido a que tomando en cuenta las evidencias encontradas, se puede sospechar que el sitio web posee una puerta trasera facilitando posibles ataques a futuro.

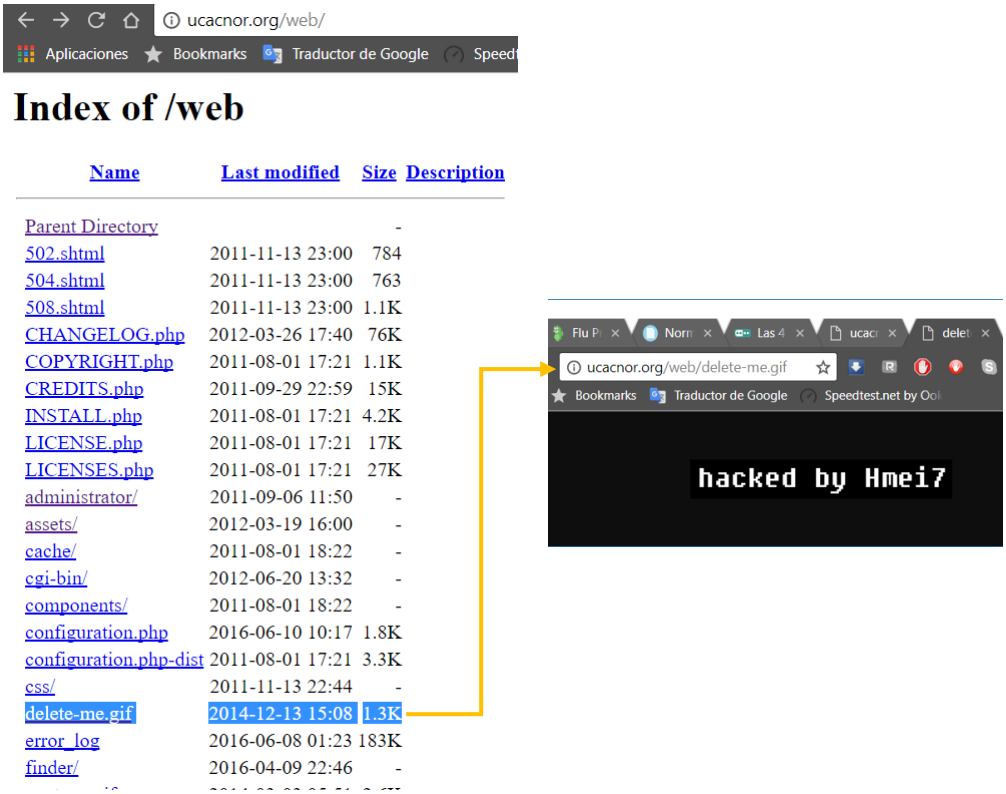
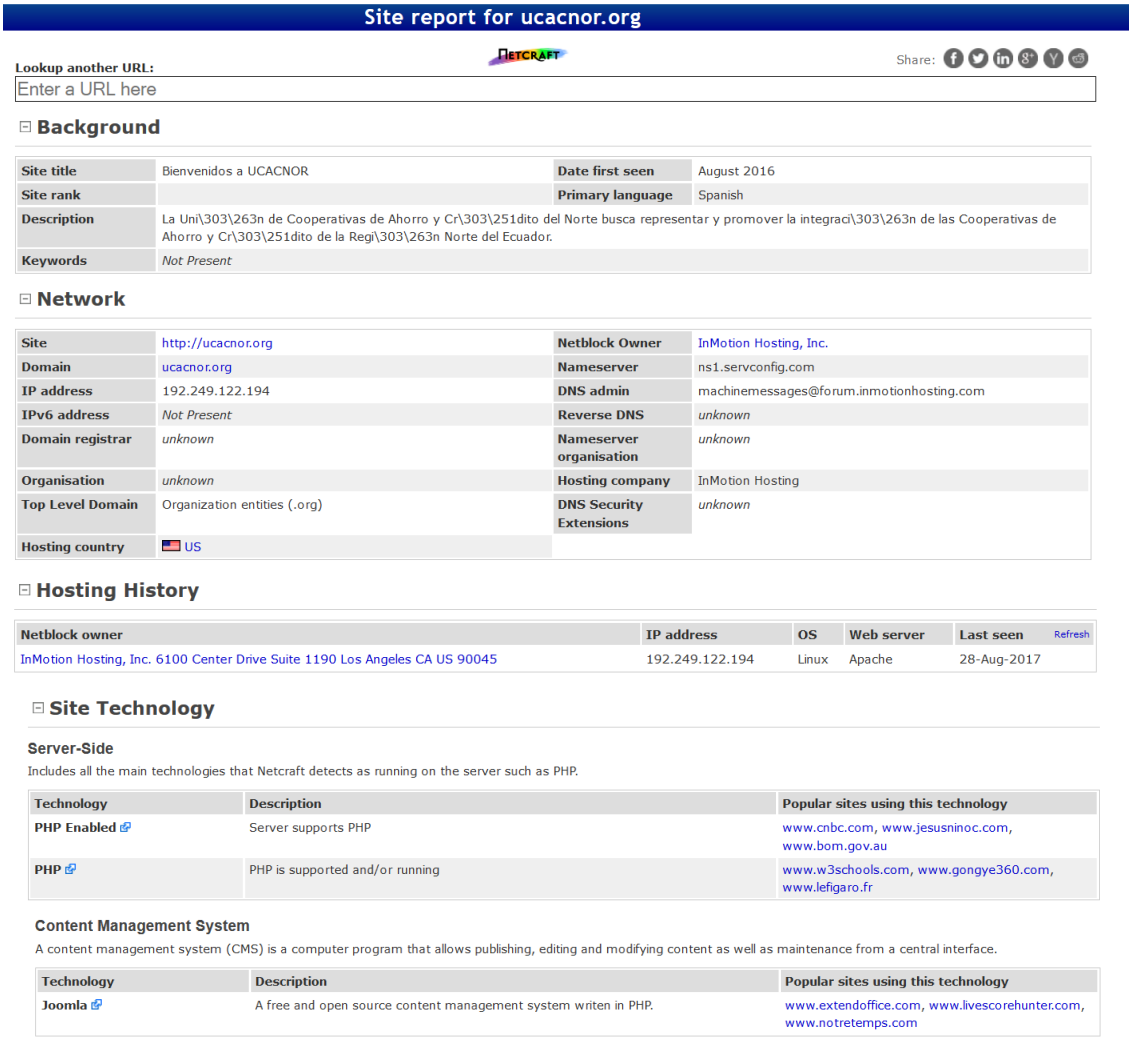


Ilustración 2.6 Evidencia de sitio web vulnerado.
Fuente: Propia.

2.1.2 PoC: Búsqueda de información pasiva

Existen varias páginas en línea y software offline para recoger información de un objetivo de forma pasiva, en este caso se utilizó la página "Netcraft" (http://toolbar.netcraft.com/site_report?url=http://ucacnor.org) en la cual se obtuvo datos muy interesantes y completos sobre el dominio a auditar, la siguiente ilustración muestra los resultados obtenidos:



Site report for ucacnor.org

Lookup another URL: Enter a URL here

Share:

Background

Site title	Bienvenidos a UCACNOR	Date first seen	August 2016
Site rank		Primary language	Spanish
Description	La Uni\303\263n de Cooperativas de Ahorro y Cr\303\251dito del Norte busca representar y promover la integraci\303\263n de las Cooperativas de Ahorro y Cr\303\251dito de la Regi\303\263n Norte del Ecuador.		
Keywords	*Not Present*		

Network

Site	http://ucacnor.org	Netblock Owner	InMotion Hosting, Inc.
Domain	ucacnor.org	Nameserver	ns1.servconfig.com
IP address	192.249.122.194	DNS admin	machinemessages@forum.inmotionhosting.com
IPv6 address	*Not Present*	Reverse DNS	*unknown*
Domain registrar	*unknown*	Nameserver organisation	*unknown*
Organisation	*unknown*	Hosting company	InMotion Hosting
Top Level Domain	Organization entities (.org)	DNS Security Extensions	*unknown*
Hosting country	US		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen (Refresh)
InMotion Hosting, Inc. 6100 Center Drive Suite 1190 Los Angeles CA US 90045	192.249.122.194	Linux	Apache	28-Aug-2017

Site Technology

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
PHP Enabled	Server supports PHP	www.cnbc.com, www.jesusninoc.com, www.bom.gov.au
PHP	PHP is supported and/or running	www.w3schools.com, www.gongye360.com, www.lefigaro.fr

Content Management System

A content management system (CMS) is a computer program that allows publishing, editing and modifying content as well as maintenance from a central interface.

Technology	Description	Popular sites using this technology
Joomla	A free and open source content management system writen in PHP.	www.extendoffice.com, www.livescorehunter.com, www.notretemps.com

Ilustración 2.7 Resultados pasivos obtenidos en Netcraft.
Fuente: Propia.

En esta prueba se logró descubrir varios datos interesantes acerca del dominio “ucacnor.org”, pero los más relevantes para el Pentesting son los siguientes:

- **Protocolo:** HTTP.
- **IP de la página web:** 192.249.122.194.
- **Sistema operativo:** Linux.
- **Servidor web:** Apache.
- **País:** Estados Unidos.
- **Proveedor de hospedaje:** InMotion Hosting, Inc.
- **Tecnología usada en la página web:** PHP.
- **Gestor de contenidos:** Joomla.

Con la información encontrada anteriormente, se puede aprovechar vulnerabilidades conocidas sobre el tipo de gestor de contenidos utilizado o sobre el servidor web identificado.

Otra herramienta online que ayuda bastante al realizar un reconocimiento pasivo es GoDaddy, la cual al realizar una búsqueda WHOIS sobre el dominio deseado, se obtiene la siguiente información:

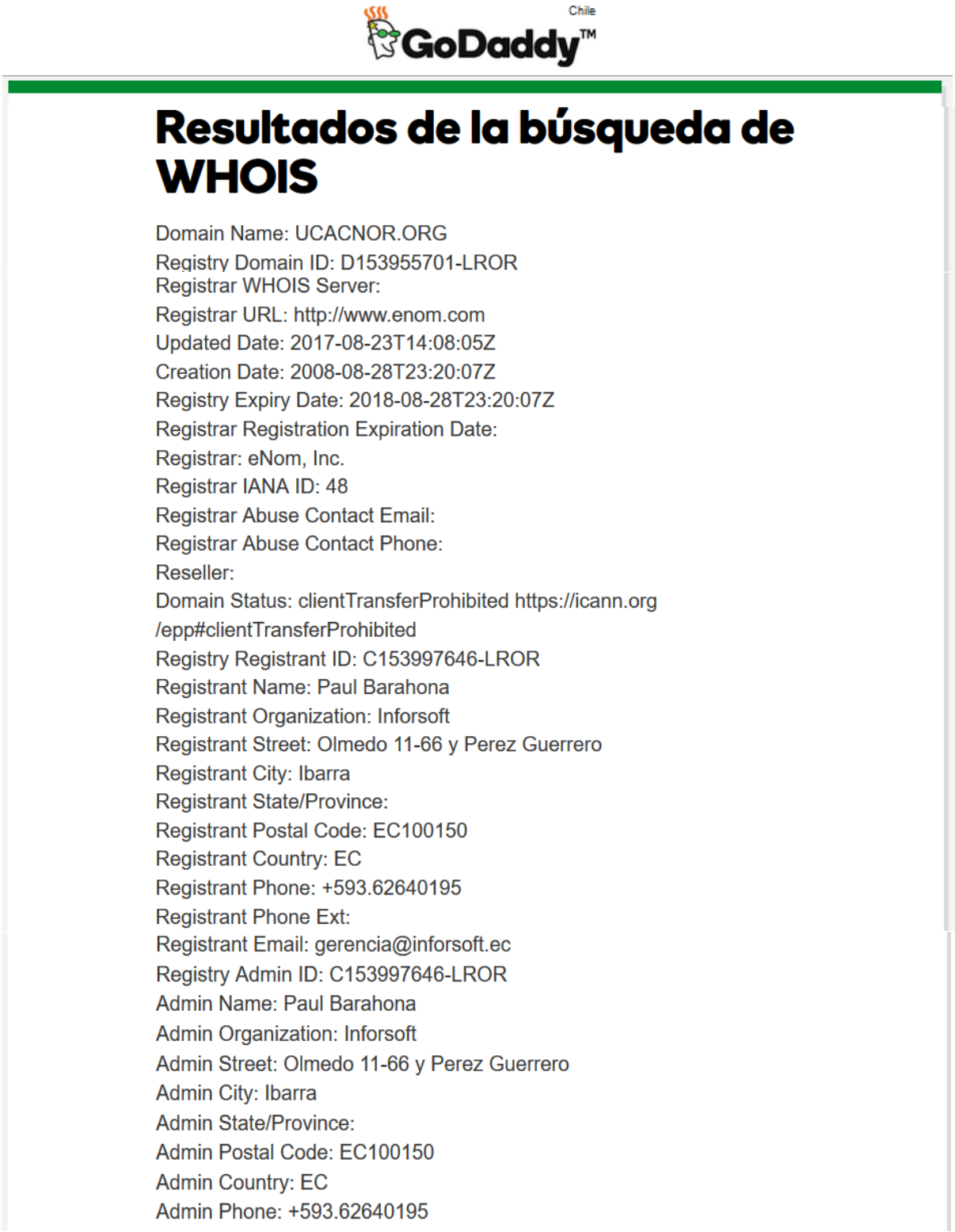


Ilustración 2.8 Información obtenida en la búsqueda WHOIS.
Fuente: Propia.

En la información obtenida anteriormente, se evidencia que la organización auditada “UCACNOR”, utiliza los servicios de una empresa externa para su página web y correo electrónico; por lo tanto, no es posible realizar pruebas agresivas que puedan afectar directa o indirectamente a la entidad encargada del hospedaje; además solo se cuenta con la autorización por parte de UCACNOR, más no de la otra empresa.

2.1.3 PoC: Versiones de página web en Internet Archive

Internet Archive o mejor conocido como “archive.org”, es un sitio de internet dedicado al almacenaje de distintos tipos de archivos a través del tiempo, uno de ellos son las páginas web, siendo posible conocer los cambios históricos que estas han tenido; para esta prueba de concepto se ha consultado la URL de la empresa auditada obteniendo como resultado más relevante, los indicios de otra posible intrusión de seguridad a su página web el 19 de marzo del 2011, la cual se muestra a continuación:

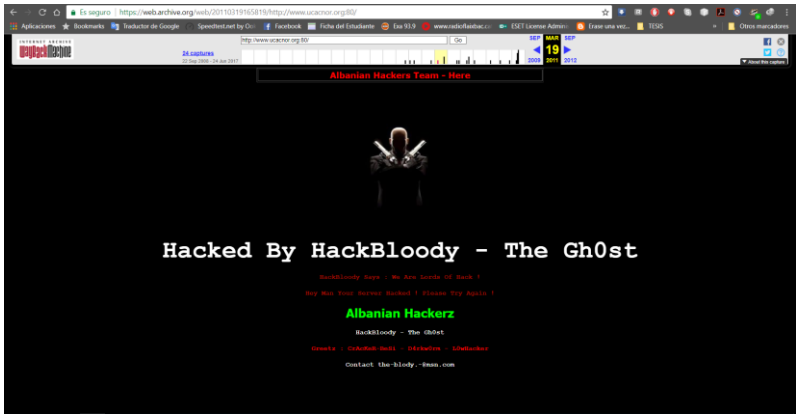


Ilustración 2.9 Captura de pantalla del registro de la página web del objetivo vulnerada.
Fuente: Propia.

2.1.4 PoC: Búsqueda de direcciones de correo con “The Harvester”

Es una herramienta muy utilizada en un test de intrusión, se ejecuta a través de un script en Linux y permite realizar una búsqueda en internet de las direcciones de correo con mayor exposición de un dominio en específico, para esta prueba se buscó las direcciones del dominio “ucacnor.org” que se encuentren muy expuestas a los principales motores de búsqueda. Se ejecutó la herramienta antes mencionada en la distribución Kali Linux como se muestra en la siguiente ilustración:

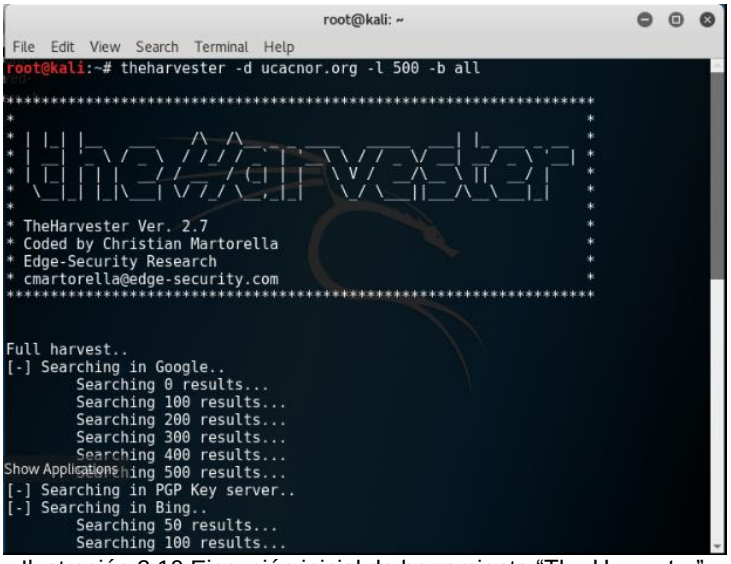


Ilustración 2.10 Ejecución inicial de herramienta “The Harvester”.
Fuente: Propia.

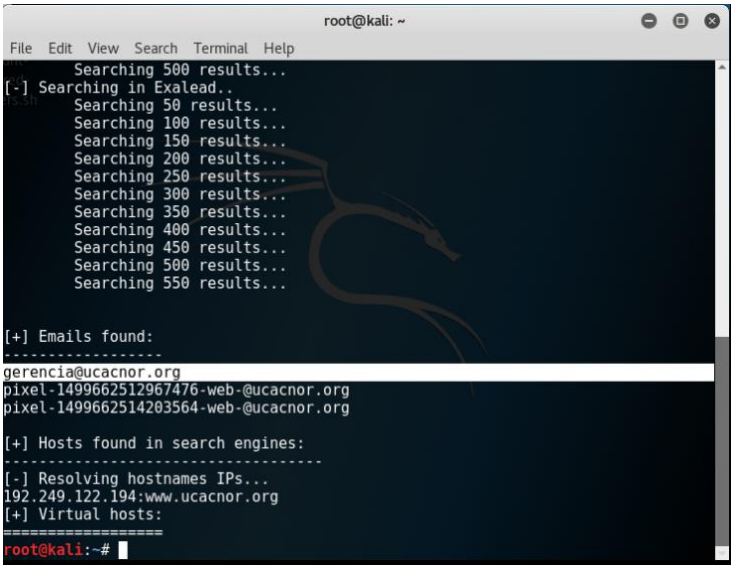


Ilustración 2.11 Resultado de herramienta “The Harvester” sobre dominio auditado.
Fuente: Propia.

Como se evidencia en la imagen anterior, la única cuenta de correo con un mayor nivel de exposición es la de “gerencia@ucacnor.org”, por lo tanto, esta posiblemente será la más atacada con spam o malware por cibercriminales, el problema principal radica en que al ser una cuenta prioritaria es casi imposible reemplazarla con otro nombre de usuario, por lo tanto, se deberá implementar mecanismos robustos de protección al servicio de correo electrónico.

2.1.5 PoC: Extracción y análisis de metadatos en sitio web

Un aspecto clave a revisar en la fase de recolección de información son los metadatos presentes en un sitio web, para lo cual se utilizó la herramienta FOCA para comprobar este aspecto en el dominio auditado.

Se inició la prueba de concepto con la creación del proyecto en el software FOCA y posteriormente se inició el escaneo al dominio “ucacnor.org” como se muestra en la siguiente ilustración:

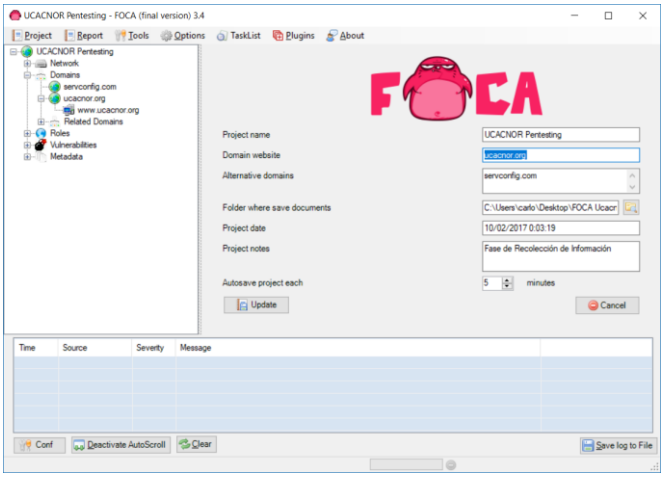


Ilustración 2.12 Creación y ejecución del proyecto en FOCA.
Fuente: Propia.

Una vez la herramienta haya terminado el escaneo, se observa en el apartado “Metadata” todos los archivos encontrados, los cuales serán analizados en busca de metadatos para posteriormente ordenar y clasificar esa información.

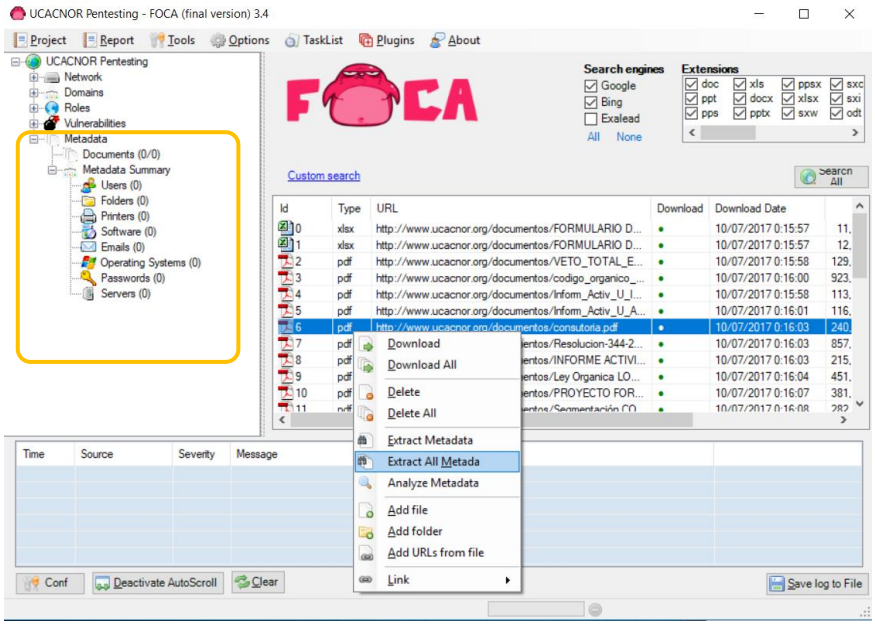


Ilustración 2.13 Documentos encontrados en el dominio auditado.
Fuente: Propia.

El análisis realizado por FOCA se encarga de ordenar y agrupar los metadatos encontrados, para posteriormente mostrarlos al usuario de la siguiente manera:

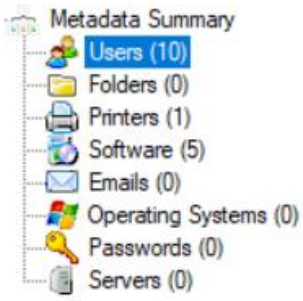


Ilustración 2.14 Resumen de los metadatos encontrados en www.ucacnor.org.
Fuente: Propia.

La extracción y análisis de metadatos presentes en el sitio web auditado muestran una cantidad considerable de información de diferentes tipos como: usuarios, software utilizado e impresoras.

Ilustración 2.15 Usuarios, impresoras y software encontrado en metadatos.
Fuente: Propia.

2.2 Fase de Enumeración

En esta etapa se continuó recogiendo información del objetivo, pero se utilizó técnicas y herramientas más intrusivas y agresivas con los activos tecnológicos de UCACNOR. Esta fase se enfocó en la identificación activa de los objetivos, mediante escaneos de puertos, identificación de servicios y sistemas operativos.

Las actividades efectuadas en esta etapa fueron:

- Búsqueda automatizada de información en sitio web.
- Acceso a la red interna.
- Detección de direcciones IP y equipos.
- Detección de DNS (Transferencia de zona).

- Detección de Servicios y sus versiones.
- Detección de WAFs en sitio web.

2.2.1 PoC: Extracción de información general con Maltego

Maltego es una herramienta gráfica multiplataforma la cual escanea todo tipo de información a un objetivo en específico, para esta prueba se utilizó la versión “Community Edition” la cual es gratuita para fines investigativos, misma que buscó información acerca del dominio auditado “ucacnor.org”.

Cabe destacar que se ejecutó todo tipo de búsquedas, las cuales el Maltego son conocidas como “transformadas”, por lo tanto, el análisis fue muy completo y consistió en la obtención de información sobre: DNS, detalles del proveedor, cuentas de correo electrónico, archivos y documentos del dominio auditado.

Ilustración 2.16 Menú de transformaciones ejecutadas en Maltego.
Fuente: Propia.

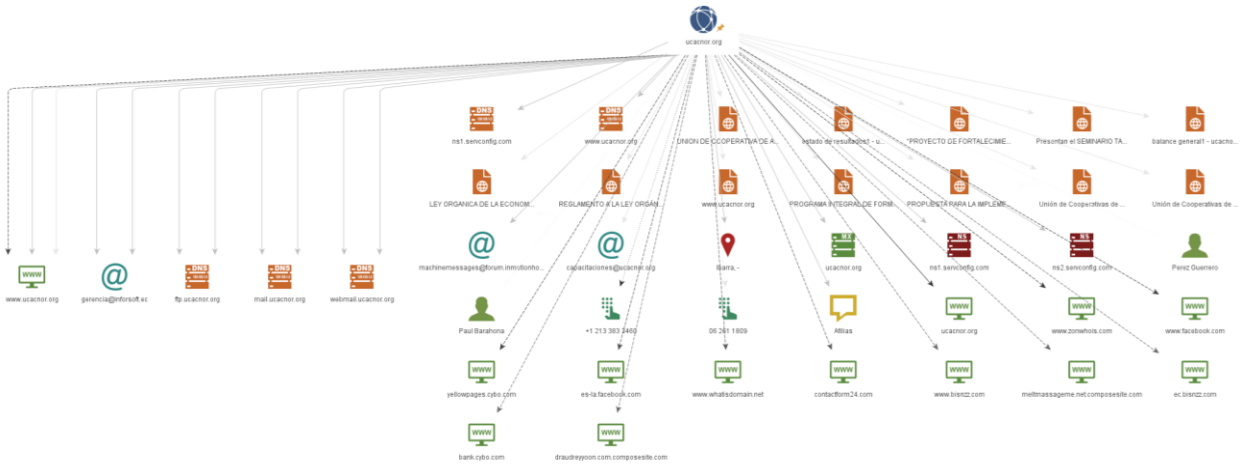


Ilustración 2.17 Información obtenida sobre el dominio objetivo.
Fuente: Propia.

La información recogida por Maltego ha sido estructurada con un diagrama de flechas, las cuales indican información muy variada como: varios correos electrónicos, el nombre de un posible servidor FTP, correos electrónicos, servidores DNS, varios documentos, una ubicación física, nombres de usuarios, números de teléfono y finalmente varios sitios web enlazados al dominio investigado.

2.2.2 PoC: Acceso a la red interna a través de router inalámbrico

Para continuar con la fase de enumeración y tomando en cuenta el acceso físico al objetivo, se vio la necesidad de vulnerar la red interna de la organización, ingresando a ella a través de sus puntos de acceso inalámbricos; para lo cual se siguió el siguiente proceso:

a) En Kali Linux, se ejecutó la terminal y se colocó la interfaz inalámbrica del equipo en modo "Monitor".

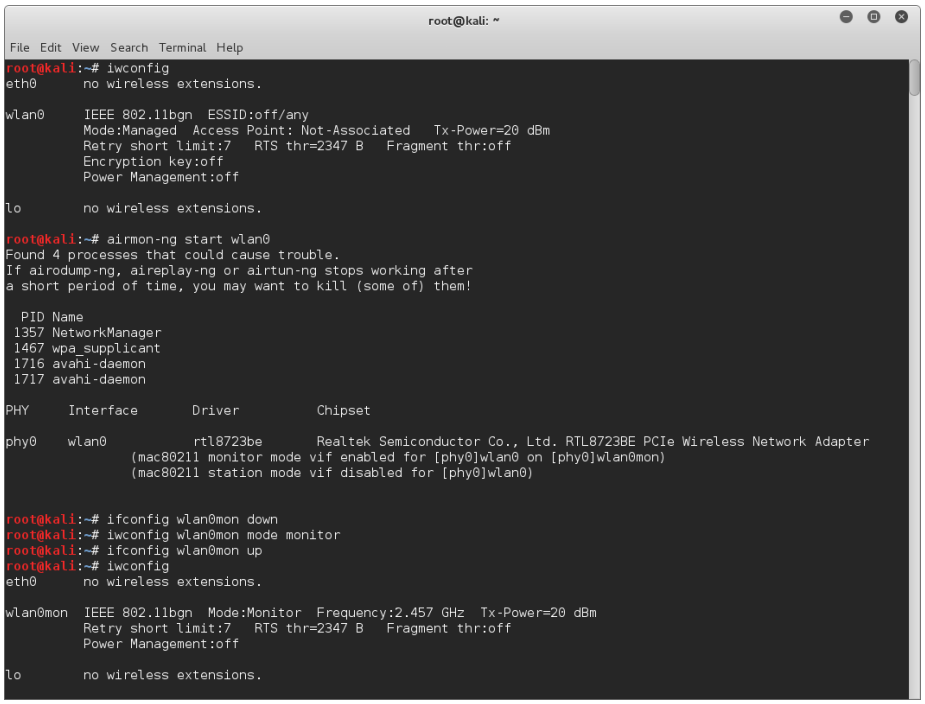


Ilustración 2.18 Inicio modo monitor.
Fuente: Propia.

b) Se escaneo las redes inalámbricas cercanas, se observó el ESSID "UCACNOR" con una dirección física y potencia muy similares al ESSID "CAPACITACIONES", por lo tanto, se concluyó que pertenecen al mismo equipo objetivo. Además, en la tabla posterior se visualizó los dispositivos conectados en ese momento a cada equipo antes listado.

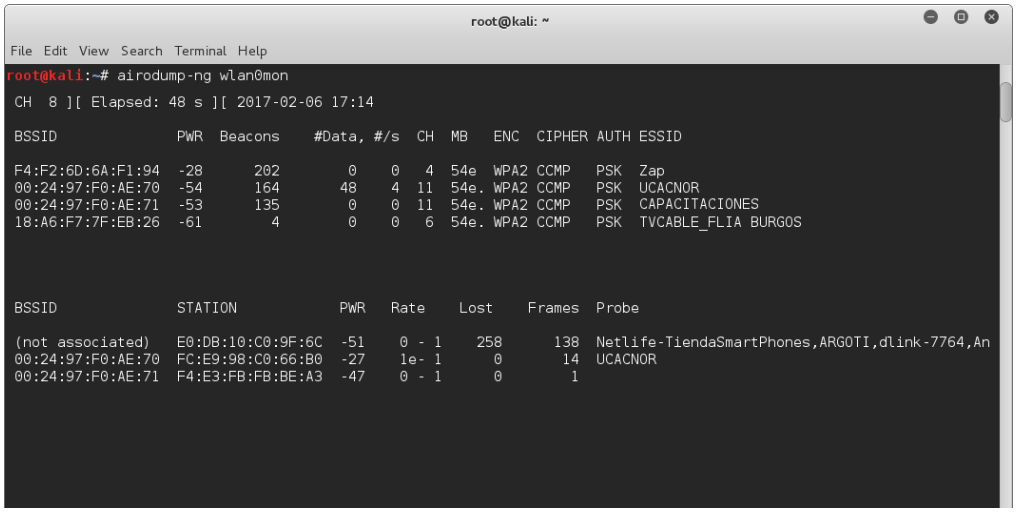


Ilustración 2.19 Escaneo de redes.
Fuente: Propia.

c) Se monitoreó la autentificación de un dispositivo con el router a vulnerar, para después capturar el *handshake* y generar el archivo de dicha captura.

Ilustración 2.20 Monitoreo de objetivo.
Fuente: Propia.

d) Se realizó un ataque de des autentificación a cualquier dispositivo conectado al router a vulnerar, con el objetivo de obtener su *handshake* mediante el monitoreo del literal anterior.

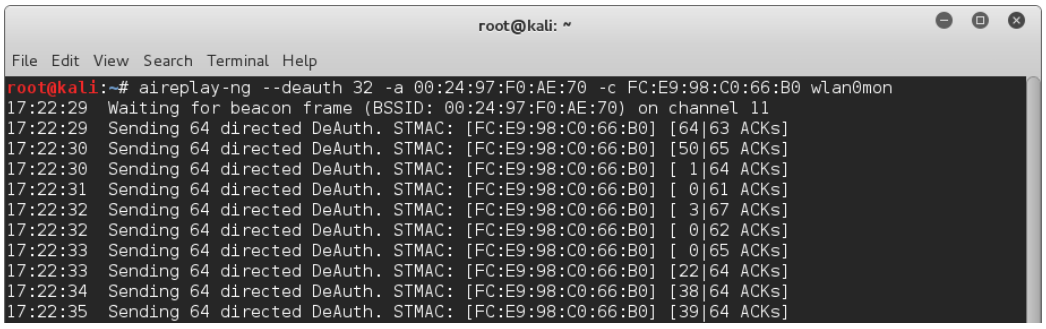


Ilustración 2.21 Ataque de des autentificación.
Fuente: Propia.

e) Posteriormente se obtuvo el *WPA handshake*, el cual es escrito en un archivo en formato "*.cap"*, el cual posteriormente será analizado.

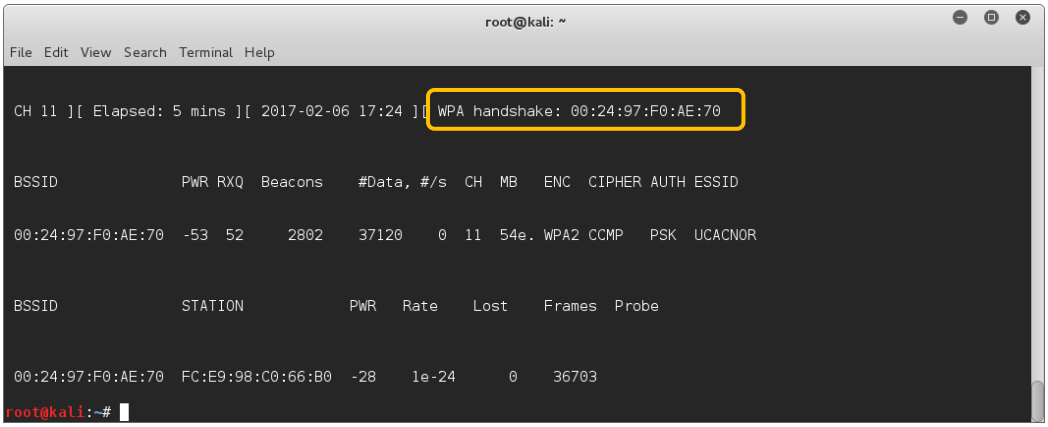


Ilustración 2.22 Obtención de handshake.
Fuente: Propia.

f) Una vez terminados los procesos anteriores, fue necesario utilizar un software que permita descifrar el archivo de captura del *handshake* antes obtenido; en este caso se utilizó la herramienta HashCat con el diccionario "rockyou". Cabe destacar que fue necesario convertir el archivo de captura del *handshake* a un formato entendible por HasCat, por lo tanto, el archivo "*.cap"* fue transformado a un archivo "*.hccapx"*, como se muestra a continuación:

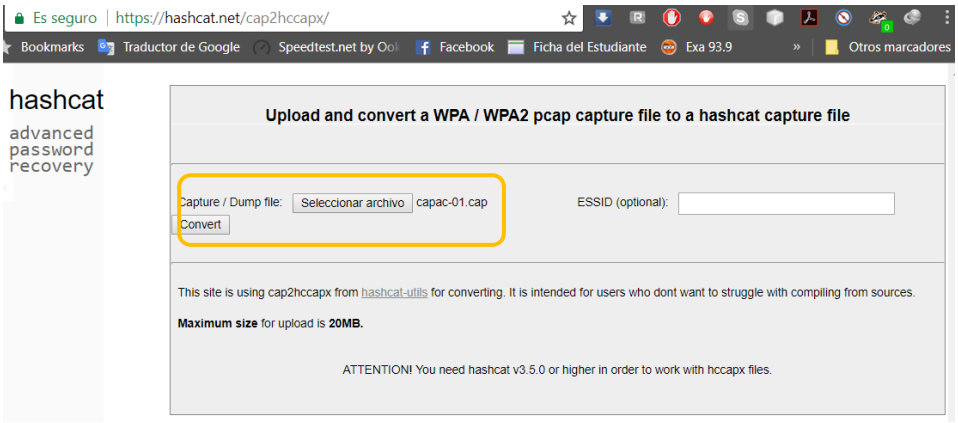


Ilustración 2.23 Conversión de formatos.
Fuente: Propia.

g) Finalmente se ejecutó la herramienta HashCat con los parámetros indicados en los puntos anteriores.

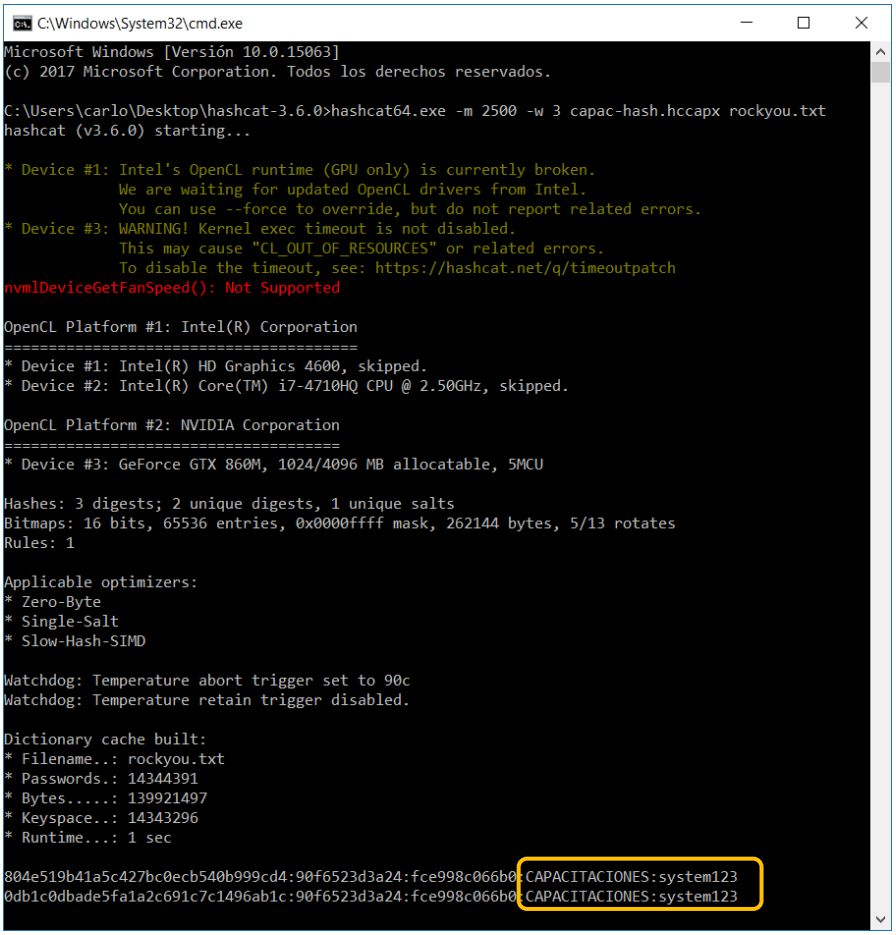


Ilustración 2.24 Ejecución de HashCat.
Fuente: Propia.

Acabado el proceso, la contraseña ha sido encontrada en el diccionario, misma que se guardará en los registros de Hashcat. Este proceso fue repetido aplicando los mismos parámetros para obtener la contraseña de la red “UCACNOR”.

2.2.3 PoC: Detección de equipos y direcciones IP.

Una vez vulnerado el acceso inalámbrico de la red interna, se ejecutó la herramienta “Wireless Network Watcher” la cual permite descubrir todos los equipos dentro de la organización con su respectiva dirección IP, MAC, nombre y compañía del adaptador de red.

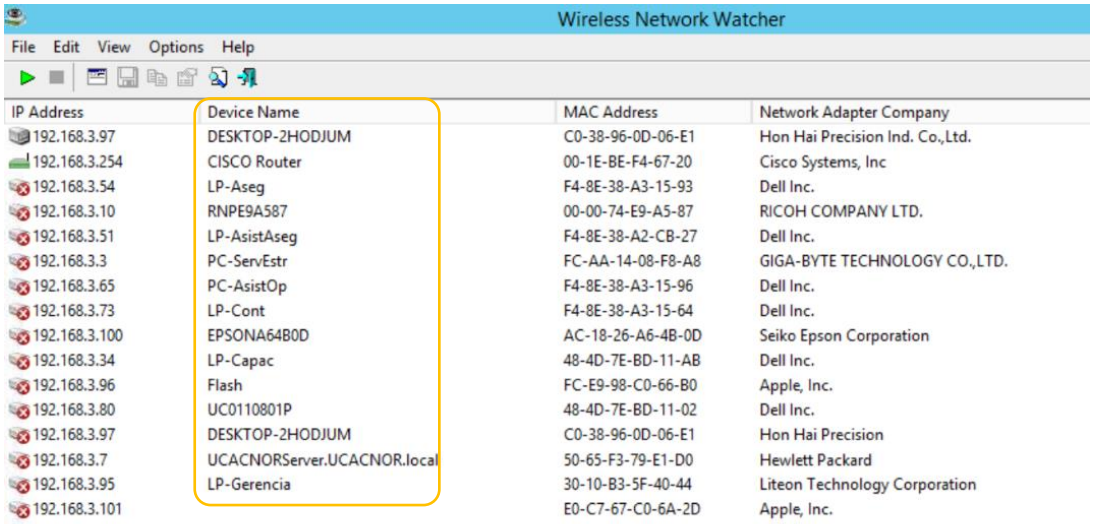


Ilustración 2.25 Detección de equipos.
Fuente: Propia.

Con esta prueba se obtuvieron los diferentes equipos y dispositivos que han sido conectados a la red interna; además, la imagen anterior expone el nombre de cada equipo encontrado, por lo que utilizando la información sobre las Unidades de UCACNOR obtenida en la primera etapa del Pentesting, se pudo asociar qué área específica posee determinado equipo; esto puede abrir la posibilidad para que un cibercriminal ejecute ataques dirigidos a personal determinado en la organización o inclusive seleccione a un empleado susceptible a ingeniería social o phishing.

2.2.4 PoC: Análisis de puertos, servicios y SO al servidor local

Uno de los activos más importantes por auditar en una organización es su servidor local, el cual alberga gran cantidad de información y servicios críticos, por lo tanto, una vez identificada la dirección IP del servidor local de UCACNOR, se efectuó el escaneo de puertos, servicios y sistema operativo con la herramienta “NMAP”.

Ilustración 2.26 Escaneo con NMAP.
Fuente: Propia.

Como se observa en la imagen anterior, existe una gran cantidad de puertos abiertos en el servidor local, lo cual puede significar un potencial vector de ataque si no se cierran los puertos innecesarios o no se actualizan los servicios vinculados a estos. Además, la prueba reveló que se está ejecutando el sistema operativo “Microsoft Windows Server” con servicios sobresalientes como: base de datos “MySQL 5.6.26”, web “Apache 2.4.16 x32” y VNC “TightVNC”.

2.2.5 PoC: Transferencia de Zona

La exposición de datos sensibles es una vulnerabilidad incluida en el informe de la OWASP TOP TEN 2017 el cual se lo describe en el Capítulo 2 de esta investigación, el cual a primera vista puede parecer con poca relevancia al momento de llevar acabo un Pentesting, pero lo cierto es que la exposición de datos sensibles puede exponer otros vectores de ataque por los cuales un atacante puede obtener información crítica de una organización.

La siguiente prueba de concepto, comprobó si el servidor primario de resolución de nombres detrás del dominio “ucacnor.org” está bien configurado, impidiendo la exposición de datos relevantes como nombres y direcciones IP de equipos de la misma zona que el servidor.

Primeramente, se detectó el equipo que aparezca en el registro SOA, la misma que poseerá el conocimiento de los nombres y direcciones IP de la zona (Aparicio de la Fuente, 2017).

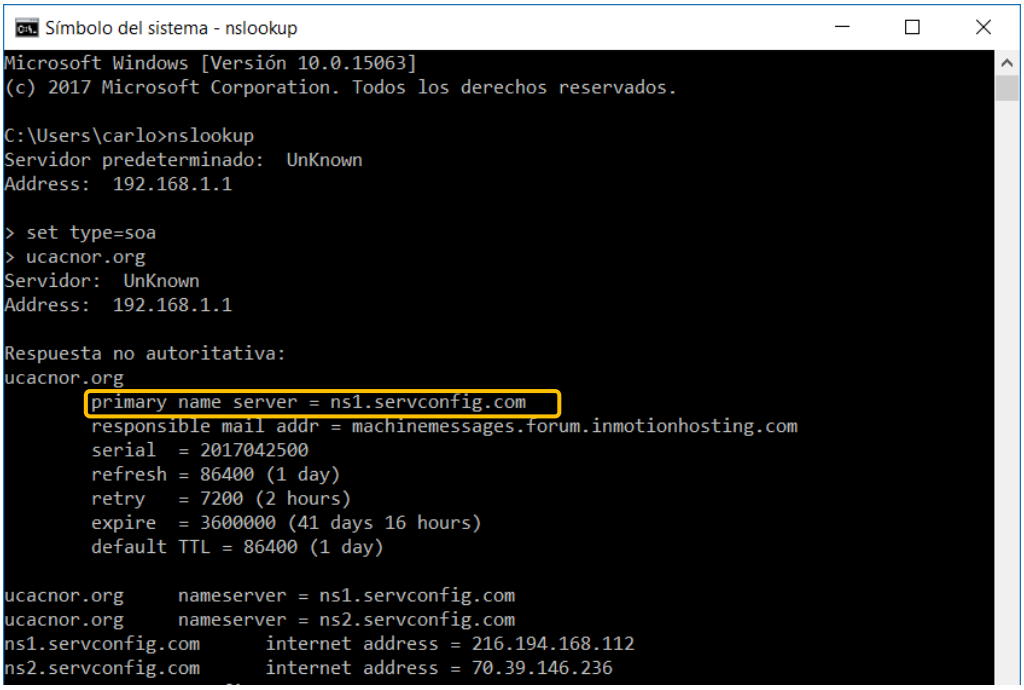


Ilustración 2.27 Comandos para prueba de concepto sobre transferencia zona.
Fuente: Propia.

Una vez que se ha expuesto el servidor primario de nombres en esta zona, se procede a configurarlo como servidor predeterminado de nombres del equipo donde se ejecuta la prueba, para posteriormente ejecutar la petición de transferencia de zona, consultándole por todos los equipos configurados con el nombre de dominio principal donde este se encuentra (Aparicio de la Fuente, 2017).

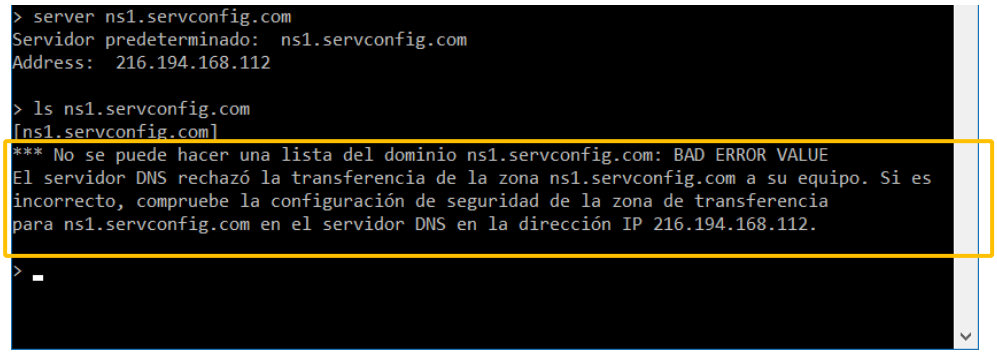


Ilustración 2.28 Rechazo del servidor DNS a prueba de transferencia de zona.
Fuente: Propia.

Si el servidor de nombres primario de la zona no está bien configurado, arrojaría todos los hostnames y las direcciones IP de las máquinas que forman la zona que él controla; en este caso se puede evidenciar que este rechazó la transferencia de zona y no expuso ninguna información, por lo tanto, se encuentra mayormente seguro.

2.2.6 PoC: Comprobación de Firewall o IDS detrás de una página web

Para verificar si existe algún equipo de seguridad protegiendo la página web de la organización que estamos auditando, se utilizó la herramienta Wafwoof de Kali, la cual envía una serie de peticiones sospechosas a un servidor web, para posteriormente analizar las respuestas obtenidas y determinar si ha existido algún tipo de bloqueo, rechazo o detección por mecanismos de defensa comúnmente conocidos como WAF (Web Application Firewall) (Nájera-Gutiérrez, 2016).

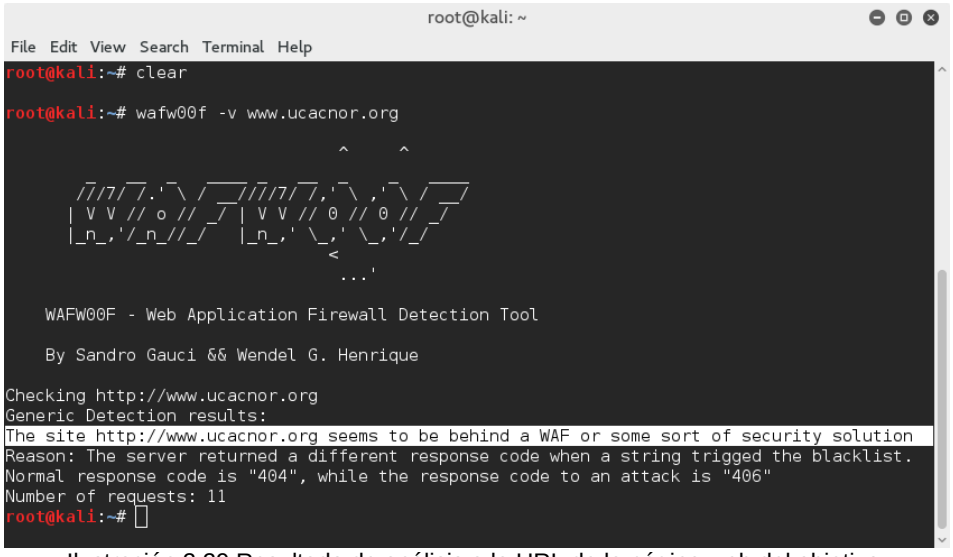


Ilustración 2.29 Resultado de análisis a la URL de la página web del objetivo.
Fuente: Propia.

Luego de realizar la prueba anterior, se evidencia que la página web del objetivo si cuenta con un mecanismo de seguridad, sin embargo, la herramienta ha generado resultados genéricos imposibilitando la identificación exacta del tipo de protección utilizado.

2.3 Fase de Análisis

En esta etapa se tuvo contacto directo y agresivo con los activos tecnológicos de UCACNOR, es decir, las pruebas efectuadas ya involucraron directamente a servidores, terminales de usuario, sitios web y redes; causando que sea posible la detección del proceso efectuado. Gracias a toda la información antes obtenida se ejecutó dos escáneres de

vulnerabilidades, uno enfocado en sitios web y otro en infraestructura tecnológica interna, además fue posible esquematizar la infraestructura tecnológica interna de la organización.

Cabe destacar que debido a que ningún servicio tecnológico auditado contaba con una metodología de auditoría propia, se continuó normalmente con las etapas indicadas en la metodología empleada.

Las actividades efectuadas en esta etapa fueron:

- Modelado de la infraestructura interna.
- Identificación de fallos conocidos, mediante escáneres de vulnerabilidades.

2.3.1 Modelado de la infraestructura interna

Gracias a la información obtenida en etapas anteriores, fue posible esquematizar la posible estructura tecnológica interna de UCACNOR, la cual desempeñará un papel complementario al momento del escaneo de vulnerabilidades.

El modelo expuesto en la siguiente ilustración muestra de forma consolidada los equipos y su distribución presente en la infraestructura interna, hasta llegar a internet.

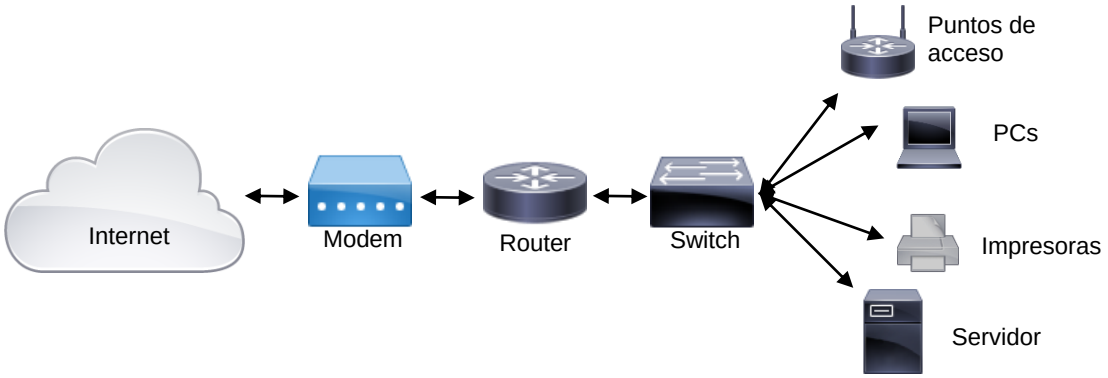


Ilustración 2.30 Esquema de la infraestructura interna de UCACNOR.
Fuente: Propia.

2.3.2 PoC: Análisis de vulnerabilidades a sitio web

Para efectuar el análisis de vulnerabilidades en el sitio web de la organización auditada, se utilizó el software “Acunetix”, el cual de una forma automatizada se encargó de comprobar si existen fallos conocidos y su respectivo nivel de criticidad; para lo cual se inició añadiendo el dominio objetivo, como se muestra en la siguiente ilustración:

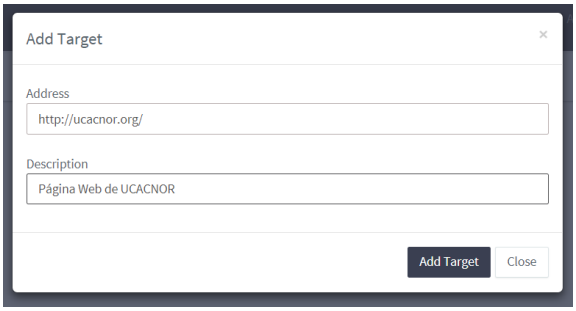


Ilustración 2.31 Ingreso de objetivo a escanear en Acunetix.
Fuente: Propia.

Posterior al ingreso inicial del escáner se procedió a ejecutarlo, el cual después de un tiempo considerable finalizó mostrando información complementaria sobre el objetivo como: datos sobre el servidor web, sitio web y direcciones web relacionadas; en la siguiente ilustración se muestran los resultados obtenidos:

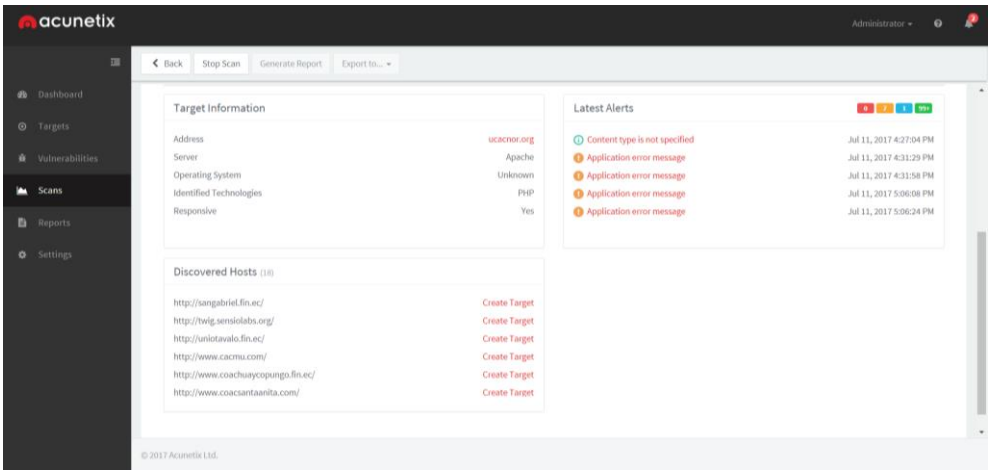


Ilustración 2.32 Resultados informativos del escaneo al sitio web.
Fuente: Propia.

En la pestaña “Vulnerabilidades” en cambio se obtuvieron los posibles fallos presentes en el sitio web, para lo cual será necesario revisarlas en la etapa de Explotación para corroborar la información obtenida. Las posibles vulnerabilidades encontradas son las siguientes:

Tabla 2.1
Posibles vulnerabilidades en sitio web

Descripción	**Severidad**
Mensaje de error de aplicación	Media
Credenciales de usuario enviadas en texto plano	Media

Formulario HTML sin protección CSRF	Media
La cabecera no posee protección X-Frame-Options anti Clickjacking	Baja

Fuente: Propia.

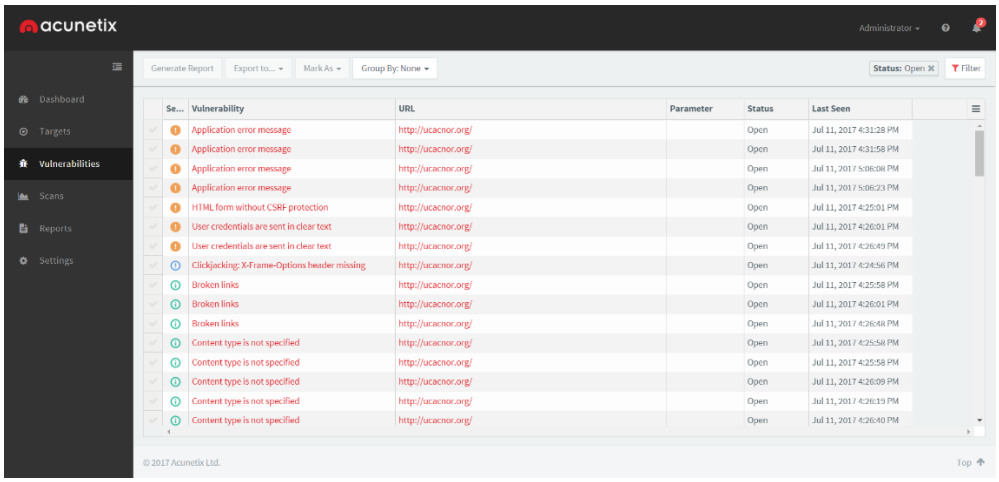


Ilustración 2.33 Posibles vulnerabilidades encontradas por Acunetix.
Fuente: Propia.

2.3.3 PoC: Análisis de vulnerabilidades a infraestructura tecnológica interna

Para complementar la Fase de Análisis del Pentesting, se ejecutó un escáner de vulnerabilidades enfocado a la infraestructura interna de una organización, en este caso se utilizó el software “Nessus Home Edition” en la distribución Kali Linux.

Una vez finalizada la instalación, se ejecutó el software y se creó una nueva Política de escaneo avanzada, como se muestra en la siguiente ilustración:

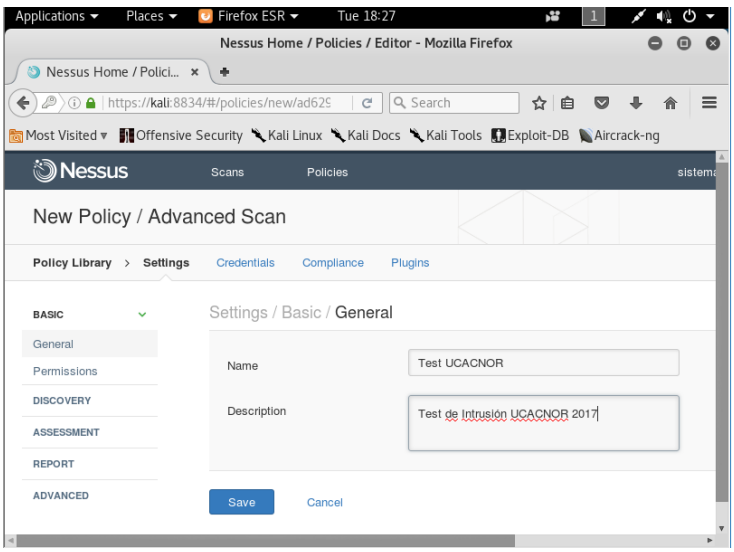


Ilustración 2.34 Creación de nueva política de escaneo avanzada.
Fuente: Propia.

Posterior a la creación y personalización de acuerdo con las necesidades propias para esta auditoría, se ejecutó el escaneó varias veces como se muestra a continuación:

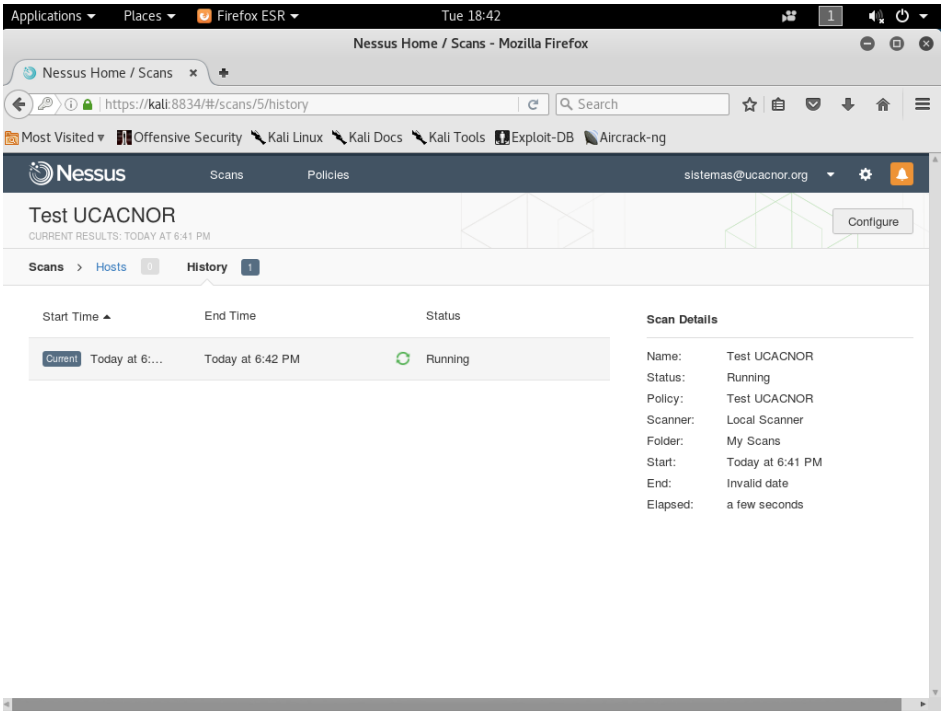


Ilustración 2.35 Ejecución del escaneo en Nessus.
Fuente: Propia.

Como se mencionó al inicio de esta fase, este escaneo fue configurado para que sea agresivo, lo cual causó que la solución de seguridad ESET Smart Security instalada en nuestro equipo mostrara varias alertas cuando el escáner estaba funcionando, por lo tanto, es muy probable que haya ocurrido lo mismo con varios usuarios dentro de UCACNOR, abriendo la posibilidad que se detecte al pentester.

Ilustración 2.36 Alerta mostrada por solución de seguridad.
Fuente: Propia.

Una vez el escaneo finalizó, el software mostró las posibles vulnerabilidades presentes en la infraestructura interna de UCACNOR, mismas que serán aprovechadas en la siguiente fase del Pentesting. Las posibles vulnerabilidades encontradas son las siguientes:

Tabla 2.2
Posibles vulnerabilidades en infraestructura interna

Descripción	**Severidad**
MS17-010 Vulnerabilidad de ejecución de código remoto (EternalBlue - DoublePulsar)	Crítica
Firmas SMB deshabilitadas	Media
Detección del servidor DHCP	Baja

Fuente: Propia.

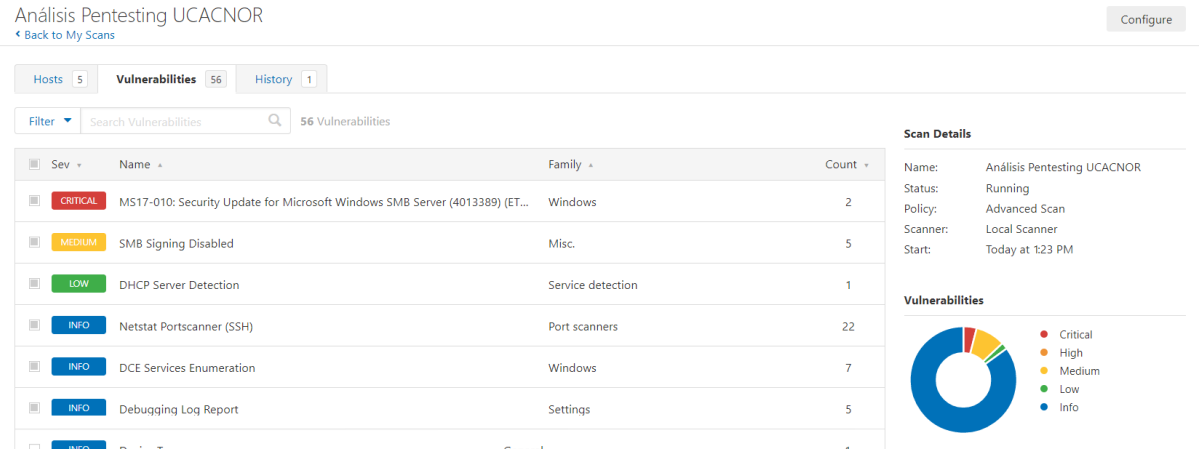


Ilustración 2.37 Posibles vulnerabilidades en infraestructura encontradas.
Fuente: Propia.

Finalizada la detección de posibles vulnerabilidades tanto en el sitio web, como en la infraestructura interna de UCACNOR, la siguiente fase del Pentesting se encargará de explotar los fallos que puedan significar una potencial amenaza para la organización.

2.4 Fase de Explotación de vulnerabilidades

En base a las posibles vulnerabilidades obtenidas en la Fase de Análisis, en esta etapa se ejecutaron ataques intrusivos y directos a un objetivo en específico, las herramientas utilizadas para llevar acabo la explotación fueron EvilFoca, Wireshark y Metasploit Framework.

Las actividades efectuadas en esta etapa fueron:

- Fuerza bruta.
- Captura de información de red.
- Búsqueda y ejecución de exploits conocidos.

- Escala de privilegios.

2.4.1 PoC: Explotación de vulnerabilidad de ejecución de código remoto

El objetivo de esta prueba es demostrar que uno de los equipos pertenecientes a la organización auditada es susceptible a la explotación de la vulnerabilidad (MS17-010) la cual permite acceder y manipular completamente el equipo. Esta debilidad es causada por un fallo de Microsoft Server Message Block 1.0 (SMBv1) de Windows. Cabe destacar que para realizar esta prueba es necesario contar con el software “WINE” instalado y configurado en Kali Linux, además la herramienta Metasploit Framework debe poseer el exploit “Eternalblue-Doublepulsar-Metasploit” encontrado en el repositorio GitHub de la empresa Eleven Paths.

El procedimiento efectuado para explotar esta vulnerabilidad fue:

a) Se inició la prueba ejecutando la consola de Metasploit Framework en Kali Linux.

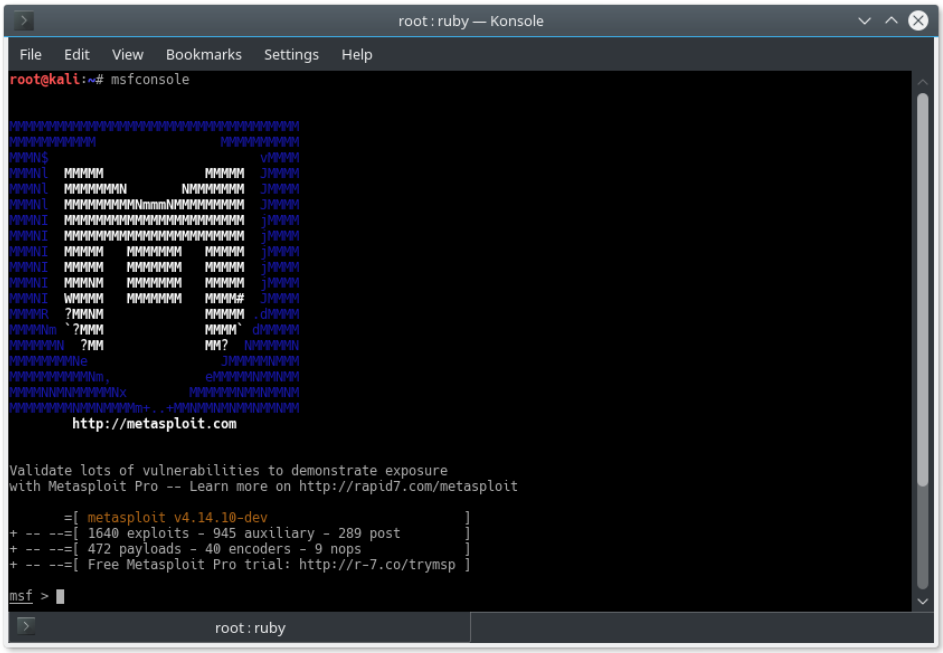


Ilustración 2.38 Consola de Metasploit Framework.
Fuente: Propia.

b) Se inició el exploit auxiliar para verificar si el equipo por atacar es realmente vulnerable a “MS17-010”. Después de haberlo iniciado, fue necesario asignar la IP (RHOSTS) de la máquina por auditar.

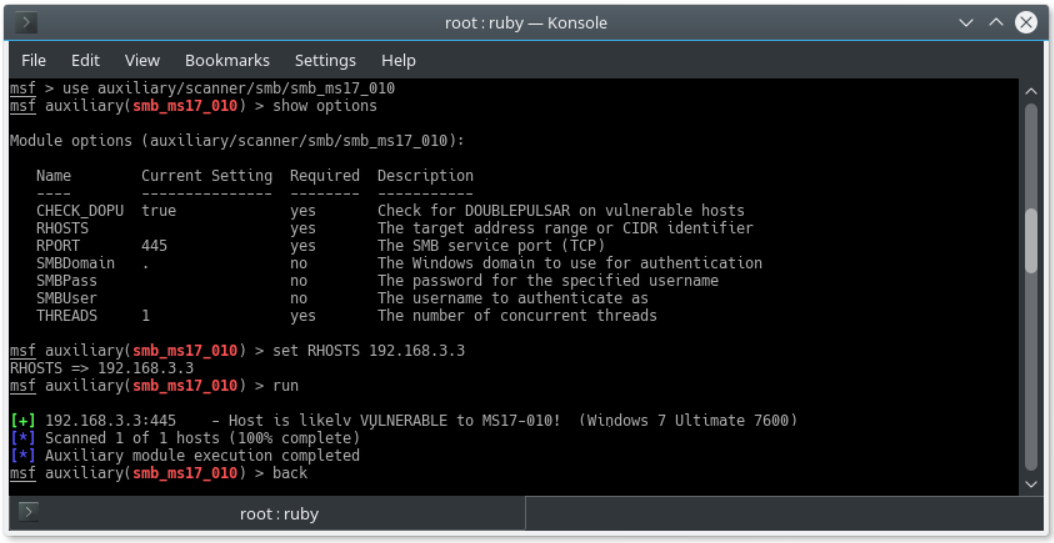


Ilustración 2.39 Ejecución de exploit auxiliar verificador.
Fuente: Propia.

c) Una vez comprobado que el equipo es vulnerable a “MS17-010”, se ejecutó el exploit “EternalBlue - DoublePulsar”, el cual es el indicado para esta vulnerabilidad específica. Las opciones que se configuraron para dicho exploit fueron:

   a. Dirección IP del objetivo: RHOST 192.168.3.3
   b. Arquitectura del objetivo: TARGETARCHITECTURE x64
   c. Proceso para inyectar al objetivo: PROCESSINJECT explorer.exe
   d. Dirección IP de escucha: LHOST 192.168.3.97

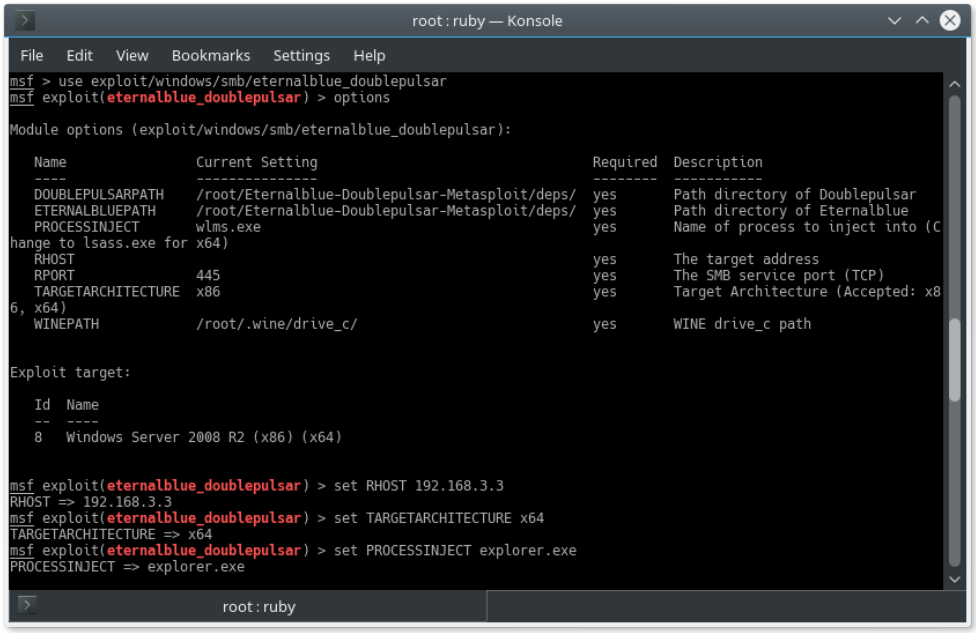


Ilustración 2.40 Configuración de opciones del exploit EternalBlue – DoublePulsar.
Fuente: Propia.

d) Se seleccionó el *payload* adecuado para este ataque en específico, se utilizó el *payload* para 64 bits que nos dio acceso al intérprete (shell) de Microsoft Windows, también se puede utilizar un *payload* para ejecutar *meterpreter* el cual se lo invocaría con el siguiente comando: “SET PAYLOAD windows/x64/meterpreter/reverse_tcp”.

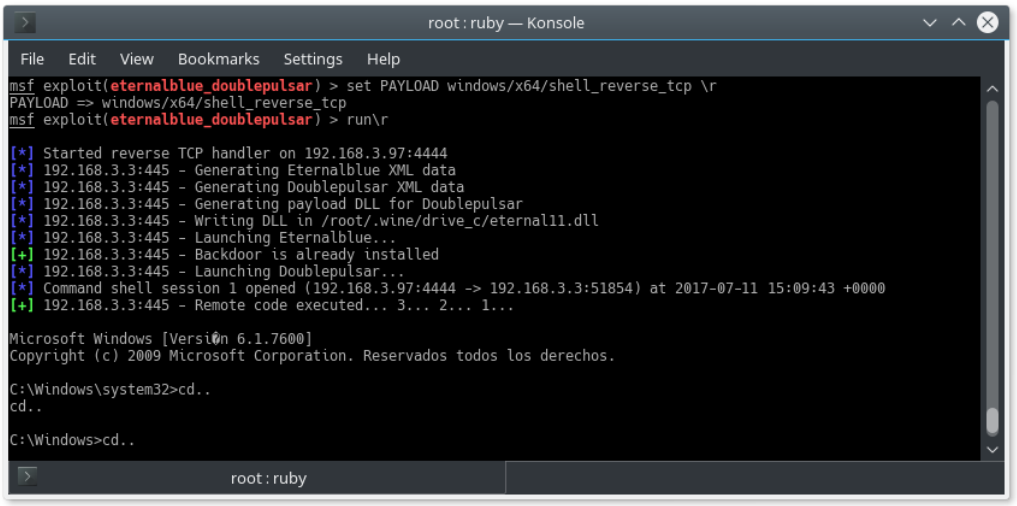


Ilustración 2.41 Ejecución del exploit EternalBlue – DoublePulsar.
Fuente: Propia.

e) Finalmente, luego de ejecutar el exploit se tuvo acceso al intérprete del sistema operativo de la máquina atacada, demostrando que la vulnerabilidad crítica detectada en la Fase de Análisis es real y explotable. Además, como se observa en las siguientes ilustraciones el exploit nos da acceso total a archivos de todos los usuarios. Para proteger los equipos de este fallo se recomienda actualizar o desactivar el protocolo Server Message Block (SMB).

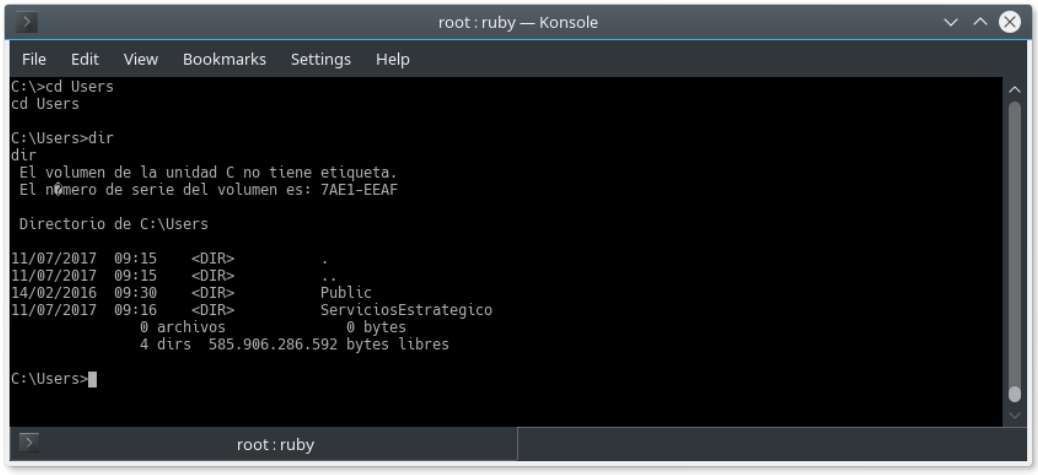


Ilustración 2.42 Visualización de carpetas de usuarios en equipo vulnerado.
Fuente: Propia.

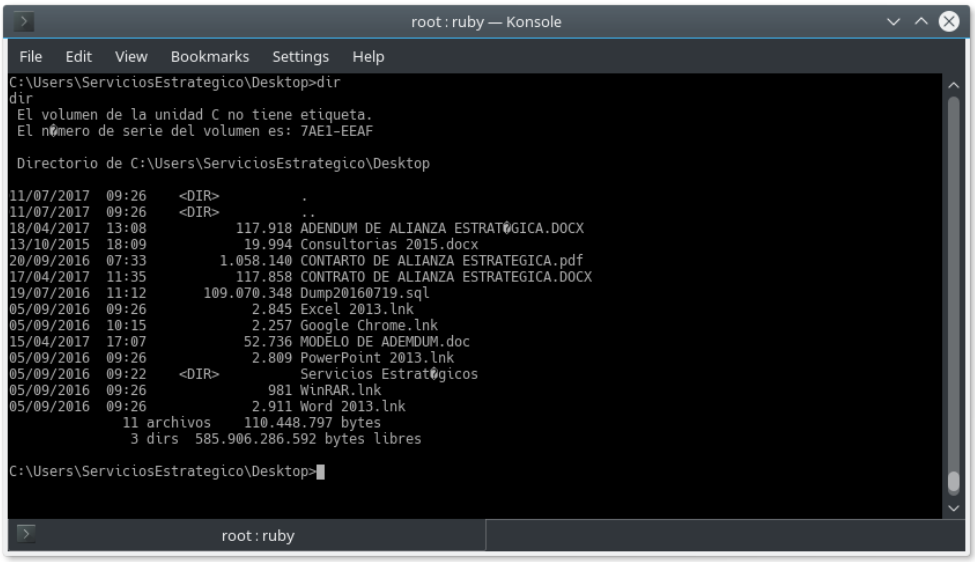


Ilustración 2.43 Visualización de archivos de usuario en equipo vulnerado.
Fuente: Propia.

2.4.2 PoC: Explotación de vulnerabilidad de captura de datos en red local

Para la siguiente prueba se utilizaron las herramientas EvilFoca y WireShark la cual tiene por objetivo ejecutar un ataque de ARP Spoofing para después interceptar los paquetes a través de la red local y de esta forma capturar credenciales enviadas en texto plano y sin encriptar al sitio web de la organización.

El procedimiento efectuado para explotar esta vulnerabilidad fue:

a) Se ejecutó el software EvilFoca el cual nos permitió realizar un ataque ARP Spoofing o envenenamiento ARP y de esta manera obtener los paquetes de red que el objetivo envía.

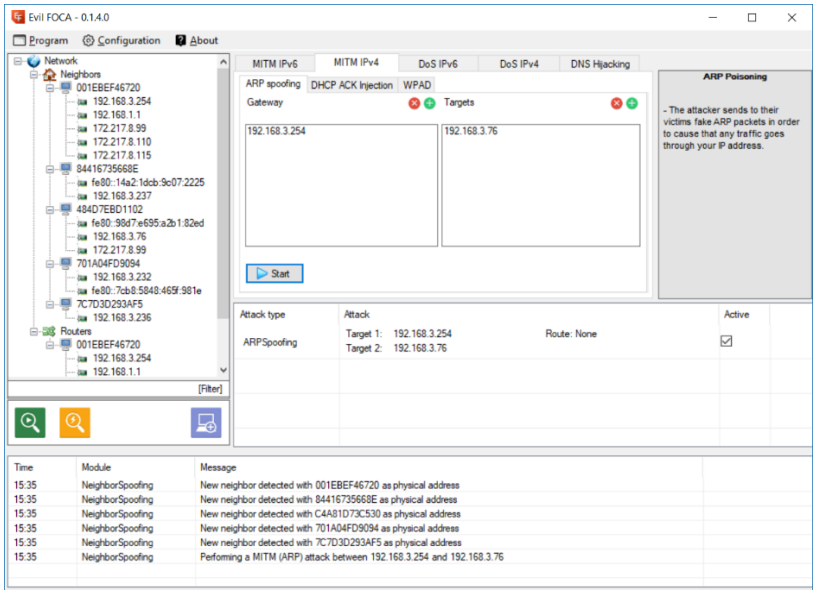


Ilustración 2.44 Ataque ARP Spoofing.
Fuente: Propia.

b) Mientras el ataque ARP Spoofing está activo, se comenzó a analizar el tráfico con la misma interfaz del ataque anterior, para después monitorear con el software Wireshark hasta que otro usuario ingrese sus credenciales institucionales, en este caso se realizó un filtro con la web a auditar “ucacnor.org”. Posterior al filtro, se buscó la palabra “administrator”, ya que en este caso se pretende interceptar las credenciales del sitio web de administración de la organización “http://ucacnor.org/*administrator*”.

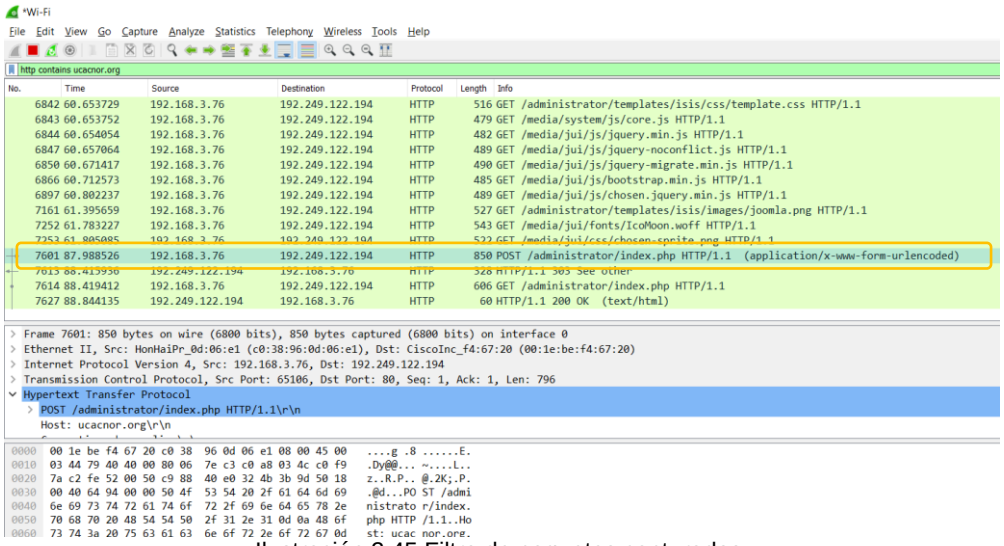


Ilustración 2.45 Filtro de paquetes capturados.
Fuente: Propia.

c) Como se observa en la siguiente imagen, el administrador de la página web ingresó al portal de la misma, dejando rastro de las credenciales de acceso utilizadas, por lo tanto, se procedió a probar las credenciales obtenidas.

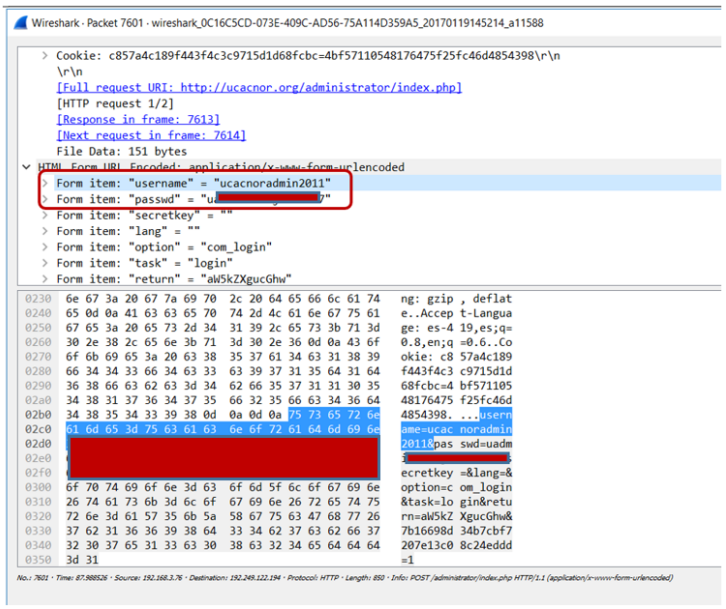


Ilustración 2.46 Credenciales en texto plano visibles.
Fuente: Propia.

d) Efectivamente se consiguió el acceso a la web de administración de la institución utilizando las credenciales obtenidas, esto demuestra la vulnerabilidad de envió de credenciales en texto plano en la página web, para proteger el sitio web de este fallo se recomienda activar el doble factor de autentificación de la plataforma.

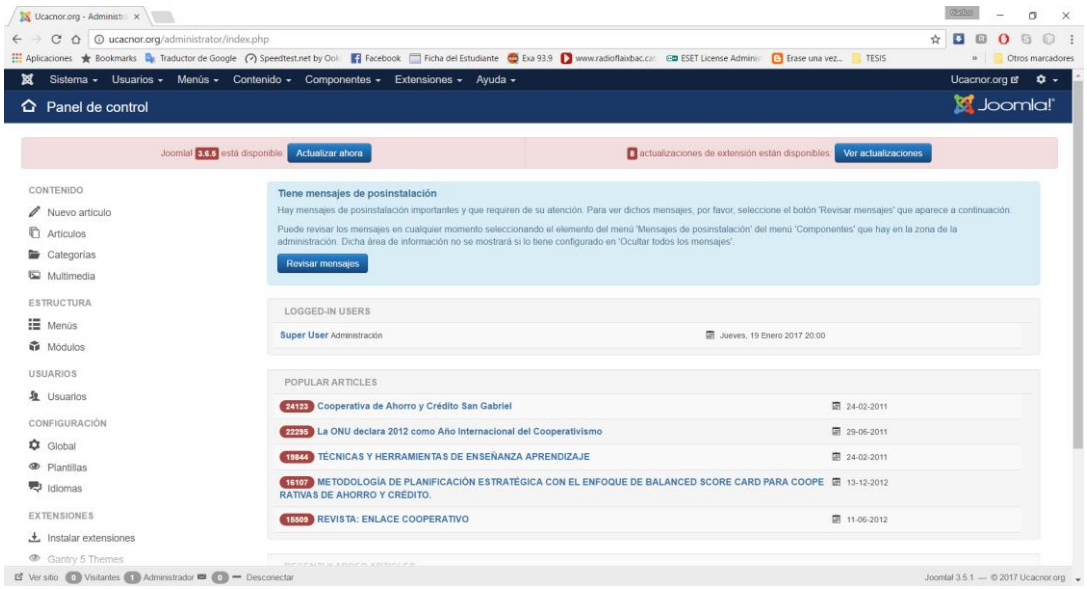


Ilustración 2.47 Ingreso a página de administración.
Fuente: Propia.

Adicionalmente, se pudo evidenciar que la página de administración del sitio web cuenta con autocompletado automático para el ingreso de usuario en el formulario de “Inicio de sesión”. También se pudo observar que el sitio web muestra información sobre su servidor y versión al momento de producirse un error.

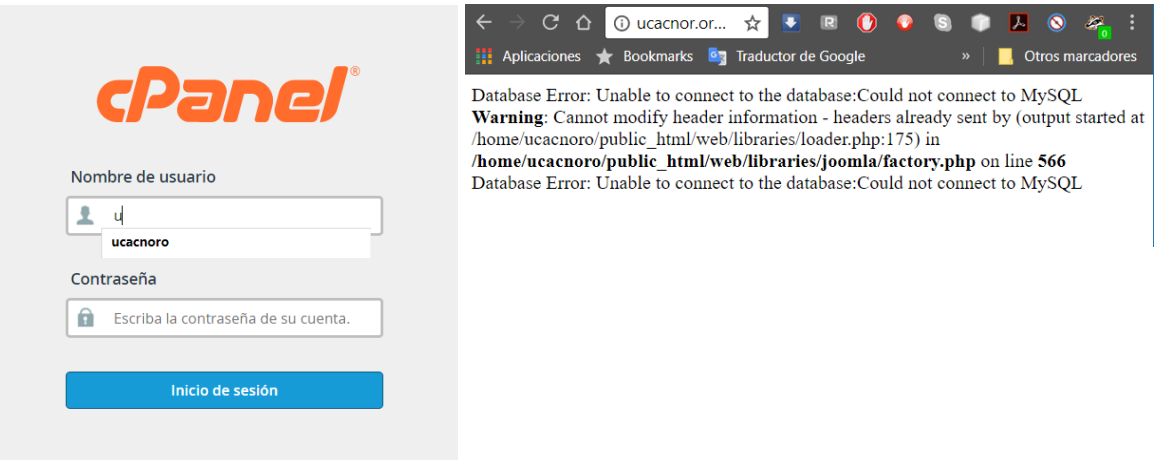


Ilustración 2.48 Vulnerabilidades de nivel bajo en sitio web.
Fuente: Propia.

2.5 Fase de Documentación

En base a las etapas anteriores y a partir de los resultados obtenidos se generó la documentación correspondiente con los detalles que comprendió la auditoría, es muy importante destacar las medidas necesarias a tomar para evitar que la organización sufra ataques reales. En esta etapa se crearon dos informes, como son el ejecutivo y el técnico; mismos que siguieron la estructura y modelo de informe propios de la organización auditada.

La estructura establecida en los informes es la siguiente:

- Portada.
- Tabla de contenido.
- Resumen.
- Justificación de la investigación.
- Objetivos
    - General.
    - Específicos.
- Desarrollo de la investigación.
    - Primera fase: Recolección de información.
    - Segunda fase: Enumeración.
    - Tercera fase: Análisis.
    - Cuarta fase: Explotación.
- Conclusiones.
- Recomendaciones.
- Firmas de responsabilidad.

Los dos informes antes mencionados cuentan con la misma estructura, con la diferencia de su contenido orientado a personas técnicas en el informe técnico y cualquier tipo de persona en el informe ejecutivo.

Los dos informes originales pueden ser encontrados en los siguientes anexos:

a) Anexo 1: Informe ejecutivo.

b) Anexo 2: Informe técnico.

CAPÍTULO 3

Resultados del Test de Intrusión o Pentesting

El Pentesting efectuado en la Unión de Cooperativas de Ahorro y Crédito del norte tuvo como objetivo principal verificar la seguridad informática en varios de sus servicios tecnológicos, para después aplicar medidas correctivas y proactivas en base a las recomendaciones que esta investigación genere; por lo tanto, una vez finalizadas todas las etapas que comprenden el Pentesting, es necesario ordenar y clasificar las vulnerabilidades encontradas.

Este capítulo expondrá las vulnerabilidades, su nivel y riesgo correspondiente encontradas en cada servicio tecnológico de la organización auditada. Posteriormente, se mostrarán varias recomendaciones para mejorar la seguridad en cada uno de los activos tecnológicos antes mencionados.

A continuación, se enlistan los activos tecnológicos auditados con su respectiva tabla de vulnerabilidades:

3.1 Vulnerabilidades en access point

Tabla 3.1
Vulnerabilidades presentes en access point.

Vulnerabilidad	Nivel de riesgo	Riesgo
Contraseñas de acceso débiles	Alto	**Acceso no autorizado e ingreso a la red interna de intrusos por ataques de diccionario y fuerza bruta**

Fuente: Propia.

3.2 Vulnerabilidades en terminales de usuario

Tabla 3.2
Vulnerabilidades presentes en terminales de usuario

Vulnerabilidad	Nivel de riesgo	Riesgo
Protocolos de Windows desactualizados y vulnerables	Crítico	**Ejecución de código malicioso remoto por medio de protocolo SMBv1**

Nombres de los equipos identificables para cada usuario	Informativo	**Identificación de equipos por usuarios inmediata en un ataque dirigido**
Privilegios de administración en todos los usuarios	Alto	**Ejecución, instalación o configuración de aplicaciones a usuarios no autorizados**
Sistemas operativos desactualizados	Alto	**Desprotección del sistema operativo a nuevas amenazas**

Fuente: Propia.

3.3 Vulnerabilidades en servidor local

Tabla 3.3
Vulnerabilidades presentes en servidor local

Vulnerabilidad	Nivel de riesgo	Riesgo
Base de datos MySql desactualizada	Medio	**Desprotección a fallos del fabricante**
Puertos abiertos innecesarios	Bajo	**Exploración y utilización no autorizada para posible acceso a información del servidor**

Fuente: Propia.

3.4 Vulnerabilidades en sitio web

Tabla 3.4
Vulnerabilidades presentes en sitio web

Vulnerabilidad	Nivel de riesgo	Riesgo
Autocompletados en páginas de inicio de sesión	Bajo	**Acceso no autorizado a administración de la página web**
Fichero “robots.txt” muestra información utilizable para realizar ataques en sitio web	Bajo	**Exposición de información sobre directorios desactivados utilizable para realizar un ataque de fuzzing en sitio web.**
Mensaje de error de aplicación web	Medio	**Visualización de mensajes de error o advertencia con posible información sensible al atacante**

Rastros forenses de ataque e intrusión anterior exitosa	Crítico	**Estructura web completa puede contener puertas traseras para posibles nuevos ataques**
Página sin protección a ataques CSRF	Medio	**Utilización de vulnerabilidades CSRF o XSRF por atacantes para dañar o robar información**
Credenciales de usuario enviadas por texto plano visibles a interceptación de comunicación	Medio	**Robo de usuarios y contraseñas por un atacante que se encuentre monitoreando la actividad de administración de la página web y correo**
Exceso de información de contacto sobre empleados publicada en sitio web de la organización	Informativo	**Posibilidad de ejecución de ataques dirigidos o ingeniería social a determinados funcionarios de la organización**
Envío de correos a cuentas de UCACNOR sin verificación de identidad real	Medio	**Engaños o fraudes por correo electrónico a funcionarios que manejen cuentas de correo institucional**
Metadatos presentes en documentos alojados en sitio web	Medio	**Extracción de información importante sobre la organización presente en archivos en sitio web**

Fuente: Propia.

Una vez expuestas las vulnerabilidades presentes en cada activo tecnológico, se emitió varias recomendaciones de mitigación con el objetivo de que la Unidad de TICs de UCACNOR sea capaz de sanearlas proactivamente y conseguir un nivel de seguridad adecuado.

3.5 Recomendaciones de mitigación

A continuación, se realizan las recomendaciones de buenas prácticas y correcciones para las vulnerabilidades encontradas en la presente investigación:

3.5.1 Red Inalámbrica (Access Point)

I. Ocultar el broadcast SSID de la red inalámbrica FUNCIONARIOS.
II. Filtrar por MAC Address cada equipo.
III. Monitoreo de nuevas conexiones en la red FUNCIONARIOS, avisó mediante correo electrónico o app movil.
IV. Deshabilitar el Protocolo DHCP en la red FUNCIONARIOS.
V. Desactivar estándar obsoleto WPS en routers inalámbricos.
VI. Fijar a la red de INVITADOS limites en ancho de banda, horario, y efectuar el cambio constante de la clave de acceso a la red.
VII. Adquisición y protección mediante reglas en el firewall a toda la red.
VIII. Realizar filtros por URL dentro de todas las redes de UCACNOR.
IX. Proteger y filtrar el correo electrónico malicioso (spam).
X. Utilizar claves robustas para el acceso a la red inalámbrica.

3.5.2 Equipos computacionales o terminales de usuario

I. Parchar las vulnerabilidades conocidas lo antes posible.
II. Mantener las actualizaciones automáticas del sistema operativo y aplicaciones siempre encendidas.
III. Seccionar el manejo de usuarios de acuerdo con sus privilegios.

3.5.3 Servidor local

I. Cerrar los puertos y recursos no utilizados.
II. Mantener actualizada la base de datos.
III. Ejecutar una política adecuada sobre generación y utilización de claves robustas en la base de datos.

3.5.4 Sitio web y correo

I. Realizar un cambio de proveedor de hospedaje de página web y flujo de correo interno, se recomienda Amazon Web y Microsoft Exchange.
II. Purgado y migración de información de la página web a nuevo proveedor de hospedaje.
III. Verificar la información pública en la página web y definir si es conveniente tenerla.
IV. Eliminar los metadatos de todo documento o archivo.

Finalmente, se puede concluir indicando que el problema y los objetivos planteados al inicio de la investigación han sido cumplidos, ya que se logró identificar las vulnerabilidades presentes en los activos pertenecientes a la organización auditada y emitir recomendaciones proactivas para la corrección de las fallas encontradas.

Conclusiones

Se realizó el estudio sobre seguridad informática en el cual se llegó a identificar las vulnerabilidades presentes en una organización, así como sus potenciales riesgos destructivos en un ambiente hostil verdadero y de esta manera tomar acciones proactivas para reducir la brecha de seguridad presente en toda empresa.

Previo al inicio de la auditoría se explicó y solicitó los permisos adecuados a las autoridades principales de la organización, con el fin de realizar un trabajo altamente ético y moral, salvaguardando el concepto de “Ethical Hacking”.

Para iniciar el Pentesting y una vez adquirido el consentimiento por parte de las autoridades gerenciales de la organización, se coordinó con la Unidad de Tecnologías de la Información y Comunicación (TICs) de dicha entidad, los servicios tecnológicos posibles para auditar, así como también las limitaciones y precauciones a tomarse.

Se evaluó el nivel de seguridad actual de los activos tecnológicos pertenecientes a la organización, lo cual permitió contar con una idea clara sobre el estado de los servicios tecnológicos en UCACNOR y si pueden perjudicar los intereses de la misma.

Al término de la investigación se generó la documentación adecuada para dar a conocer los resultados obtenidos a las partes interesadas en la organización; mismos que deberán tomar las acciones correctivas en base a las recomendaciones indicadas en dicha documentación.

Recomendaciones

Para realizar una investigación sobre seguridad informática de cualquier tipo y que esta implique la utilización de varios sistemas operativos, es recomendable utilizar instalaciones nativas en máquinas reales, debido a que las máquinas virtuales en la mayoría de los casos generan problemas o imprevistos al momento de ejecutar sistemas operativos invitados, reduciendo el tiempo valioso en una auditoría.

Se recomienda utilizar una metodología que evite borrar los rastros de la auditoría efectuada, debido a que las metodologías empleadas por cibercriminales reales se basan principalmente en la ocultación de huellas e indicios, por lo tanto, se convierte en un trabajo poco ético y muchas de las veces ilegal.

Se recomienda efectuar Tests de Penetración con frecuencia, debido a que las amenazas y vulnerabilidades de seguridad están en constante mutación y descubrimiento, obligando a las empresas a fijarse cada vez más en una de las áreas más descuidadas durante décadas.

Referencias

Acunetix. (2017). *Acunetix*. Obtenido de https://www.acunetix.com/

Alonso, C. (2013). *Pentesting con FOCA* (Primera ed.). Madrid: 0xWORD Computing S.L.

Alonso, C. (29 de Noviembre de 2015). *SlideShare.* Obtenido de https://www.slideshare.net/chemai64/cybercamp-2015-low-hanging-fruit?ref=http://www.elladodelmal.com/2015/11/do-basics-elimina-el-low-hanging-fruit.html

Alonso, C. (14 de Abril de 2017). *Un informático en el lado del mal*. Obtenido de http://www.elladodelmal.com/2017/04/publicada-owasp-top-ten-2017-release.html

Alonso, C., & Rando, E. (Septiembre de 2015). *Hacking de Aplicaciones Web: SQL Injection.* 0xWord.

Aparicio de la Fuente, A. (3 de Julio de 2017). *Blog: Un Informático En El Lado Del Mal*. Obtenido de http://www.elladodelmal.com/2017/07/un-pentesting-usando-owasp-top-ten-2017.html

AVAST Software s.r.o. (2015). *Avast*. Obtenido de https://www.avast.com/es-es/c-online-threats

Catoira, F. (24 de Julio de 2012). *ESET*. Obtenido de WeLiveSecurity: http://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

CISCO Systems. (2015). *CISCO*. Obtenido de http://www.cisco.com/c/en/us/about/security-center/virus-differences.html#2

Cluley, G. (10 de Junio de 2014). *We Live Security*. Obtenido de https://www.welivesecurity.com/la-es/2014/06/10/todo-sobre-ransomware-guia-basica-preguntas-frecuentes/

Corletti Estrada, A. (2016). *Seguridad en Redes.* Madrid: DarFE Learning Consulting, S.L.

DAIT Seguridad Informática. (14 de Octubre de 2015). Seguridad informática vs Seguridad de la información. Monterrey, Nuevo León, México. Obtenido de https://www.youtube.com/watch?v=Z2aF4UqHKkA

DragonJAR Soluciones y Seguridad Informática S.A.S. (2015). *Educación: DragonJAR*. Obtenido de https://www.dragonjar.education/curso/como-se-realiza-un-pentest/#

González Pérez, P. (2014). *Ethical Hacking Teoría y Práctica para la realización de un Pentesting* (Primera ed.). Madrid: 0xWORD Computing S.L.

González Pérez, P. (2014). *Metasploit para Pentesters* (Tercera ed.). Madrid: 0xWORD Computing S.L.

González Pérez, P., Sánchez Garcés, G., & Soriano de la Cámara, J. M. (2015). *Pentesting con Kali 2.0.* Madrid: 0xWORD Computing S.L.

Lyon, G. (2015 de Noviembre de 2015). *Nmap*. Obtenido de https://nmap.org/7/

Molina, J. (15 de Junio de 2016). *ESET*. Obtenido de WeLiveSecurity: http://www.welivesecurity.com/la-es/2016/06/15/diferentes-visiones-pentest/

Nájera-Gutiérrez, G. (2016). *Kali Linux Web Penetration Testing Cookbook.* Birmingham: Packt Publishing Ltd.

Panda Security. (2017). *Panda*. Obtenido de http://www.pandasecurity.com/homeusers/security-info/cybercrime/others/

Paus, L. (5 de Enero de 2016). *WeLiveSecurity*. Obtenido de https://www.welivesecurity.com/la-es/2016/01/05/4-alternativas-gratuitas-a-kali-linux/

Pérez, P. G. (19 de Abril de 2015). *Pentesting con PowerShell.* 0xWord. Obtenido de Microsoft: https://blogs.technet.microsoft.com/ponicke/2007/04/19/seguridad-informatica-un-poco-de-historia/

Ponemon Institute. (5 de Mayo de 2014). *Ponemon Institute.* Obtenido de https://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

Porolli, M. (4 de Septiembre de 2013). *We Live Security*. Obtenido de https://www.welivesecurity.com/la-es/2013/09/04/hashcat-funcionamiento-herramienta-mas-poderosa-para-descifrar-contrasenas/

Rando, E., González, P., Aparicio, A., Martín, R., & Alonso, C. (2016). *Hacking Web Technologies* (Primera ed.). Madrid: 0xWORD Computing S.L.

Raymond, E. S. (19 de Julio de 2015). *The Cathedral and the Bazaar*, 1.50. Obtenido de http://www.catb.org/~esr/faqs/hacker-howto.html

SoftDoit. (2016). *SoftwareDoit*. Obtenido de https://www.softwaredoit.es/definicion/definicon-gusanos.html

Telefónica Digital España. (22 de Mayo de 2015). *Eleven Paths*. Obtenido de https://www.elevenpaths.com/es/labstools/foca-2/index.html

Tenable Inc. (2017). *Tenable*. Obtenido de https://www.tenable.com/products/nessus-vulnerability-scanner

The OWASP Foundation. (2017). *OWASP.* Obtenido de https://www.owasp.org/images/3/3c/OWASP_Top_10_-_2017_Release_Candidate1_English.pdf

Weidman, G. (26 de Marzo de 2014). *Penetration Test.* San Francisco. Obtenido de http://seguridadydefensa.com.ec/informes/el-origen-de-los-virus-informaticos-9633.html

Anexos